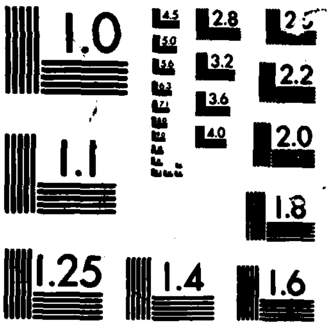
AD-A167 052 SELECTED COMPARISONS OF DEFENSE PACKET SWITCHING VS COMMERCIAL DATA COMMUNICATIONS PROTOCOLS(U) AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH J E TARANTINO 1/2

UNCLASSIFIED 1985 AFIT-CI-NR-86-57T F/G 17/2 NL



MICROCOP' CHART

1

AD-A167 052

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
AFIT/CI/NR-86-57T

2. GOVT ACCESSION NO.

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
Selected Comparisons of Defense Packet Switching vs. Commercial Data Communications Protocols.

5. TYPE OF REPORT & PERIOD COVERED
THESIS/DISSERTATION

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
James E. Tarantino

8. CONTRACT OR GRANT NUMBER(s)

9. PERFORMING ORGANIZATION NAME AND ADDRESS
AFIT STUDENT AT:
University of Colorado

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
AFIT/NR
WPAFB OH 45433-6583

12. REPORT DATE
1985

13. NUMBER OF PAGES
113

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)

15. SECURITY CLASS. (of this report)
UNCLASS

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES
APPROVED FOR PUBLIC RELEASE: IAW AFR 190-1

Lynn Wolaver 17 Apr 86
LYNN E. WOLAVER
Dean for Research and
Professional Development
AFIT/NR, WPAFB OH 45433-6583

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

57

Abstract

The Department of Defense (DOD) has mandated the use of specific protocols for use in DOD computer network systems.

The concept of this thesis is to examine some functional differences between specific DOD and industry protocols. A comparative study is used to determine how far apart the DOD is from industry standards, and if the DOD has unique requirements that are actually increasing procurement complexities and overall system costs.

A total of six protocols were selected and compared. These DOD protocols were the Defense Data Network's (DDN) X.25, the Internet Protocol (IP), and the Transmission Control Protocol (TCP). The three industry protocols were CCITT's X.25, the Connectionless-made Network Protocol (CLNP), and the Transport Protocol, Class 4 (TP-4).

The comparative study between DDN X.25 and CCITT X.25 showed that the DOD has based DDN X.25 on a widely accepted industry protocol, CCITT X.25. By using a protocol based on CCITT X.25, the DOD can implement four important concepts. These concepts are the ability to adapt to new technology, to maintain and support present systems, to decrease system costs, and to interlink separate computer systems.

The comparative study between IP, TCP, CLNP, and TP-4 showed that the DOD was not using protocols based on international standards. Six DOD operational areas were studied. These operational areas were survivability, security, precedence, robustness, equipment availability, and interoperability. Two other areas studied were affordability and technological advancements. Overall, it was shown that the DOD could begin to base its protocols on industry standards and reduce procurement times and system costs.

57

SELECTED COMPARISONS OF DEFENSE PACKET SWITCHING VS. COMMERCIAL DATA COMMUNICATIONS PROTOCOLS

by

James E. Tarantino

Capt., USAF, Thesis-113 pages

A thesis submitted to the
Faculty of the Graduate School of the
University of Colorado in partial fulfillment
of the requirement for the degree of
Master of Science
Program in Telecommunications
1985

BIBLIOGRAPHY

BBN Communications Corporation. (1983). *Defense data network X.25 host interface specification* (Research Rep. No. AD/A137 427). Cambridge, MA: Author.

CCITT X.25. (1984). *Document AP VIII-58-E. VIIIth Plenary Assembly, June 1984*.

CCITT X.224. (1985). Red Book, Vol. VIII. *Transport protocol specifications for open system interconnection for CCITT applications*. ITU Geneva.

Committee on Computer-Computer Communication Protocols. (1985). *Transport protocols for Department of Defense data networks*. Washington, DC: National Academy Press.

DIS 8473, International Organization for Standardization.

FIPS PUB 100/Federal Standard 1041 (1983). *Interface between data terminal equipment and data circuit-terminating equipment for operation with packet-switched data communications networks*. Washington, DC: National Bureau of Standards.

Internet protocol. (1983). (Standard No. MIL-STD-1777). Washington, DC: Department of Defense.

Mitre Corporation. (1984). *Defense data network system description* (Contract No. F19628-84-C-0001). McLean, Virginia, Author.

Stallings, W. (1985). *Data and computer communications*. New York: Macmillan.

Stallings, W. (1985). *Tutorial: Computer communications: Architectures, protocols, and standards*. Silver Spring, MD: IEEE Computer Society Press.

System Development Corporation. (1982). *DoD protocol reference model* (Research Rep. No. 7172/201/01). Santa Monica, CA: Author.

Tanenbaum, A. S. (1981). *Computer networks*. Englewood Cliffs, NJ: Prentice-Haall.

Telnet protocol. (1984). (Standard No. MIL-STD 1782). Washington, DC: Department of Defense.

Transmission control protocol. (1983). (Standard No. MIL-STD-1778). Washington, DC: Department of Defense.

SELECTED COMPARISONS OF DEFENSE PACKET SWITCHING VS. COMMERCIAL DATA COMMUNICATIONS PROTOCOLS

by

James E. Tarantino
B.A., Chapman College, 1980

A thesis submitted to the
Faculty of the Graduate School of the
University of Colorado in partial fulfillment
of the requirement for the degree of
Master of Science
Program in Telecommunications
1985

This Thesis for the Master of Science Degree by

James E. Tarantino

has been approved for the

Program in Telecommunications

by

Frank S Barnes

Frank S. Barnes

Harvey M. Gates

Harvey M. Gates

Dorothy M. Cerni

Dorothy M. Cerni

Date Dec 2, 1985

Tarantino, James E. (M.S., Telecommunications)

Selected Comparisons of Defense Packet Switching vs.
Commercial Data Communications Protocols

Thesis directed by Professor Frank S. Barnes

The Department of Defense (DOD) has mandated the use of specific protocols for use in DOD computer network systems. The use of these protocols could create DOD networks that may not be able to respond to advancements in technology in a timely manner and may increase procurement complexities and overall system costs.

The concept of this thesis is to examine some functional differences between specific DOD and industry protocols. A comparative study is used to determine how far apart the DOD is from industry standards, and if the DOD has unique requirements that are actually increasing procurement complexities and overall system costs.

A total of six protocols were selected and compared. These DOD protocols were the Defense Data Network's (DDN) X.25, the Internet Protocol (IP), and the Transmission Control Protocol (TCP). The three industry protocols were CCITT's X.25, the Connectionless-made Network Protocol (CLNP), and the Transport Protocol, Class 4 (TP-4).

The comparative study between DDN X.25 and CCITT X.25 showed that the DOD has based DDN X.25 on a widely accepted industry protocol, CCITT X.25. By using a protocol based on CCITT X.25, the DOD can implement four important concepts. These concepts are the ability to adapt to new technology, to maintain and support present systems, to decrease system costs, and to interlink separate computer systems.

The comparative study between IP, TCP, CLNP, and TP-4 showed that the DOD was not using protocols based on international standards. Six DOD operational areas were studied. These operational areas were survivability, security, precedence, robustness, equipment availability, and interoperability. Two other areas studied were affordability and technological advancements. Overall, it was shown that the DOD could begin to base its protocols on industry standards and reduce procurement times and system costs. The DOD has elected not to use the industry protocols, but the DOD will wait for these protocols to be completely tested and used by industry. This implication may cause procurement cycles and system costs to increase in the long run.

ACKNOWLEDGEMENTS

I would like to thank my wife, Charlotte, because without her exceptional support this thesis would never have been completed. Also, my children, James and Robert, were especially understanding during the weeks and weekends in which I spent working on the thesis.

A special thanks goes to Debra Gundersen Kelley, my sister-in-law, whose help was invaluable in completing the thesis on time. I would like to thank Dorothy Cerni who gave more time than she had in giving me extremely constructive criticism. Also, I appreciate the encouragement that Dr. Gates and Professor Barnes gave me during the research and completion of this thesis.

CONTENTS

CHAPTER

FIGURES

Figure

TABLES

Table

CHAPTER I

INTRODUCTION

The Department of Defense (DOD) has mandated the use of specific protocols for use in DOD computer network systems. The use of these protocols could create DOD networks that may not be able to respond to advancements in technology in a timely manner, potentially causing technology lags that will slow the DOD's ability to take advantage of new technologies, thus rendering networks old before their time. In addition, the more specific the needs of the DOD become, the longer the procurement cycle can take, thereby decreasing the ability of the DOD to keep up with those changes in technology. These possibilities point to the adviseability of the DOD being more closely aligned with industry in protocol designs, which would better allow the DOD to take advantage of industry changes as they come about.

The overall concept of this thesis is to examine some functional differences between the DOD and industry protocols. A comparative study between particular protocols is used to determine how far apart the DOD is from industry standards, and if the DOD has unique requirements that are actually increasing procurement complexities and overall system costs.

For the comparative study, a specific Defense Department network has been selected. A similar commercial network has not been used; rather, specific international protocol standards have been chosen for the study. The large number of protocols used by the DOD has precluded an in-depth analysis of all of them. Therefore, only specific protocols are considered in this thesis.

The Defense Department network chosen for this study is a new packet-switched network called the Defense Data Network (DDN). This network provides users with data communication services and also provides a medium over which heterogeneous computer systems can interoperate.

This thesis explores three DOD protocols being used in the DDN to determine the extent of the differences between them and ones used as standards within industry. The DOD protocols are DDN X.25, DOD's Internet Protocol (IP) and the DOD's Transmission Control Protocol (TCP). DDN X.25 is a data terminal equipment (DTE) to data circuit-terminating equipment (DCE) interface protocol. This protocol has been modeled after an international standard developed by the International

Telegraph and Telephone Consultative Committee (CCITT) called CCITT X.25. DOD's other two protocols IP and TCP are compared to the Connectionless-mode Network Protocol (CLNP) of the International Organization for Standardization (ISO) and a transport layer protocol of the Open System Interconnection Reference Model (OSI). The OSI model was developed jointly by ISO and the CCITT.

In order to follow a logical approach, the second chapter of the thesis will give an overview of the DDN and its functions, capabilities, and network components. Next, chapter three will look at the network access protocols, highlighted by a comparative study between DDN X.25 and CCITT X.25. In chapter four, a comparison is made between the two DOD protocols IP and TCP, and ISO's CLNP and a transport layer protocol of the OSI Reference Model. The final chapter gives the conclusion sought by this thesis.

CHAPTER II

DEFENSE DATA NETWORK

The Defense Data Network (DDN) is a data communications network that will provide users with both data communication services and a medium over which heterogeneous computer systems can interoperate. It will supply long-haul and area data communication services using ARPANET packet-switched technology. It will also allow the interoperability of major Command, Control and Intelligence (C^2I) systems, leading eventually to a totally integrated network.

The DDN is an extension of ARPANET technology. ARPANET was started in 1969 by the Defense Advanced Research Projects Agency (DARPA). ARPANET was originally an experimental packet-switched network used for sharing computer resources (Mitre Corp., 1983). As the network matured and met experimental requirements, it was opened to a wide community of users.

As military requirements changed, the need for an expanded system became obvious. AUTODIN II and the DDN were two experimental systems being looked at by the Defense Department. Finally, on 2 April 1982, the Deputy Secretary of Defense directed the Director of DCA to proceed with the development of the DDN (DDN Program Management Plan). The remainder of this chapter gives an overview of the DDN. It includes the DDN development, some of its capabilities and functions, and finally the needs of the users of the DDN.

2.1 Development of the DDN

The DDN will incorporate some existing command and control networks and integrate them with new networks to create a dual backbone design. The dual backbone will consist of a classified segment and an unclassified segment until higher level encryption devices allow for the combining of both segments.

The DDN will develop both segments using three existing networks. The following list contains a brief description of those networks:

1) World-Wide Military Command and Control System Intercomputer Network (WIN) - The WIN provides TOP SECRET information services at high speed data communication rates to its subscribers;

2) Advanced Research Projects Agency Network (ARPANET) - ARPANET is a research and development packet-switched network designed by the government. It is the first packet-switched network ever used, military and civilian included;

3) Movement Information Network (MINET) - MINET is an unclassified information network.

Two new networks will also be incorporated into the DDN. The following is a brief description of those networks:

1) Strategic Air Command Digital Information Network (SACDIN) - SACDIN is a multi-level secure communications network that can support subscribers with access ranging from unclassified to TOP SECRET levels;

2) Department of Defense Intelligence Information System (DODIIS) - The DODIIS supplies SCI level service to members of the intelligence community.

There will be times when top secret and secret users will require the services of the DDN. Therefore, the DDN will provide a TOP SECRET and SECRET Level in a addition to the networks that have already been discussed.

To create the dual backbone design, all the networks were split up into two separate segments. Figure 2.1 shows how ARPANET was split into ARPANET and a Military Network (MILNET) and how MILNET was joined with MINET to form the unclassified segment of the DDN. ARPANET continues to be a research and development facility under the Defense Advanced Research Projects Agency (DARPA).

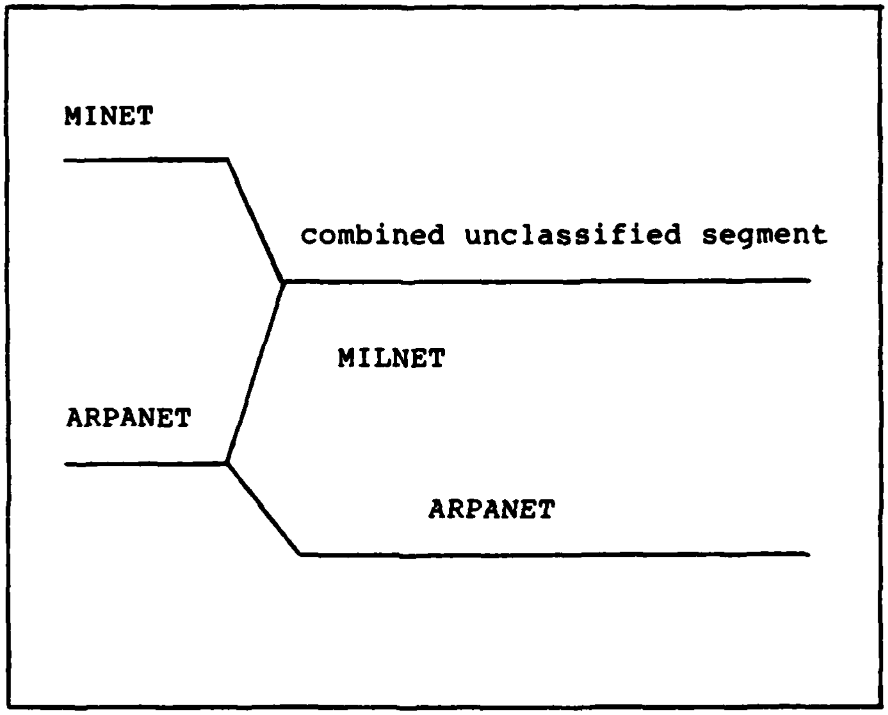


Figure 2.1 Unclassified segment of DDN

Source: Mitre Corp., 1984

The classified segment is more complex and will require integration of the remaining networks. The existing WIN, SACDIN, and DODIIS networks will eventually combine to form the classified DDN, along with the addition of the SECRET and TOP SECRET levels. Figure 2.2 shows how the integration of the separate networks will take place. The resulting C^2I network will form the classified backbone of the DDN.

The two segments will eventually combine to produce an overall secure network. Presently, when accessing the unclassified segment, an identification number is required. The number allows a user to access the DDN through his or her host computer. Access can be done through a personal computer or terminal at home using a standard modem. This concept is not very secure in the sense that anyone knowing the ID number of an individual could access the unclassified segment.

In the classified segment, the requirements for access are much more stringent. The access terminals are inside a secure area. The security level of the area is as high or higher than the terminals it is protecting. An individual wanting access must have the proper clearance and a reason to be in the secure area. Next, the user must have an additional access code in order to use the DDN. These factors make it almost impossible for someone without prior knowledge or experience of the

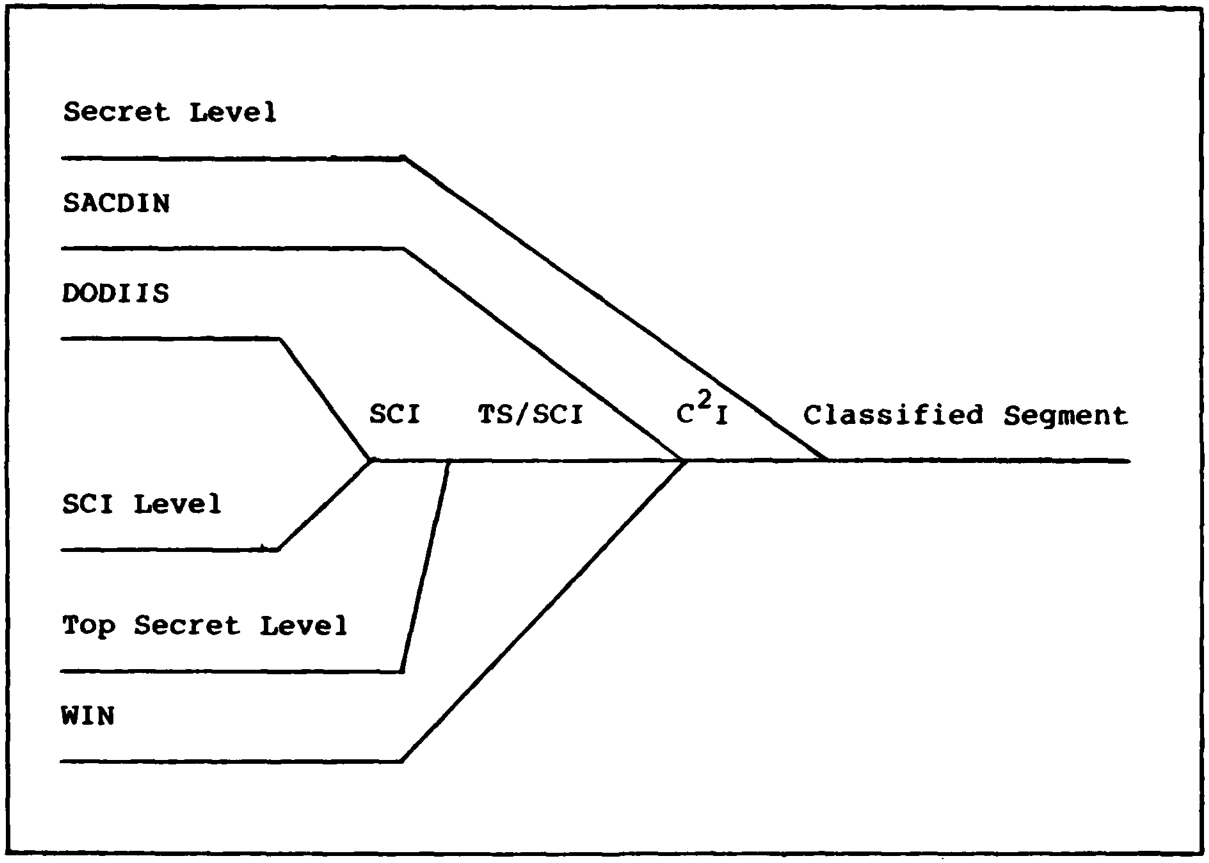


Figure 2.2 Classified segment of DDN

Source: Mitre Corp., 1984

classified network to be able to access the DDN.

Eventually, the availability of National Security Agency (NSA)-developed BLACKER equipment will allow the two segments of the DDN to be combined into one operating system. But since BLACKER technology is classified, the concept of using this technology cannot be discussed. The long-term goal is to allow additional users onto the system, such as the Inter Service/Agency Automatic Message Processing Exchange (I-S/A AMPE). These subnetworks will use the DDN as their backbone system.

2.2 DDN System Components and Functions

The DDN can be broken down into two functional segments. The long-haul data transfer segment and the local data transfer segment.

2.2.1 Long-haul Segment

The long-haul segment consists of packet switches and various transmission links to those switches. The packet switches themselves are Bolt Beranek and Newman (BBN) C/30 minicomputers that have a modular architecture to permit a variety of configurations (Mitre Corp., 1984). The BBN C/30 is considered the Interface Message Processor (IMP) in the long-haul data transfer segment and must perform a number of specific operations. The IMP is capable of adaptive routing; that is, it will not have a dedicated route or virtual circuit for its individual packets, called datagrams, but instead will be able to dynamically route datagrams separately according to network congestion or damage. In order to do this, the switch is capable of segment disassembly, packet transmission, packet receipt, packet reassembly and packet routing. The IMP will also handle precedence and preemption along with an authentication capability. Another important function of the IMP is its ability to accept specific interface protocols. Originally, Bolt Beranek and Newman Inc. (1981) designed two specific interfaces for ARPANET. These protocols, 1822 and 1822L, are used to interface a host or distant host with an IMP. The present requirements are for all new subscribers to the DDN to use a newer interface protocol called DDN X.25. This protocol has been specificlly designed for use in the DDN and is modeled after an international interface protocol from the International Telegraph and Telephone Consultative Committee (CCITT). The protocol is called CCITT X.25. DDN X.25 and CCITT X.25 are both Data Terminal Equipment (DTE) to Data Circuit-Terminating Equipment (DCE) interface protocols.

The present DOD policy for the use of DDN X.25 is that all new systems and systems being redesigned will use the DDN X.25 Protocol for interfacing with the DDN

(Air Force Information Systems Architecture, 1985). This thesis will only cover the X.25 protocols since the 1822 and 1822L protocols are being phased out.

The remainder of the long-haul system is made up of various transmission systems. Dedicated common-carrier circuits, satellite, and terrestrial circuits are normally used as transmission links to connact the packet switches.

2.2.2 Local Segment

The local segment is composed of various systems that will interface with the backbone long-haul segment. In order for these systems to operate and interface, specific hardware and software designs have been implemented. Depending on the user's capability, certain Network Access Controllers (NAC's) will be available; Figure 2.3 shows a simplified version of the DDN architecture and accompaning Network Access Controllers. These NAC's are presently being developed by the Aydyn Monitor Corp., in Fort Washington, Pennsylvania (DDN Newsletter, 1985). One NAC available now is the Terminal Access Controller (TAC) which can support asynchronous transmission only. The TAC has up to 63 ports available. The mini-TAC being developed will support synchronous or asynchronous transmission using up to 16 terminal ports. Both the TAC's and mini-TAC's will also support the

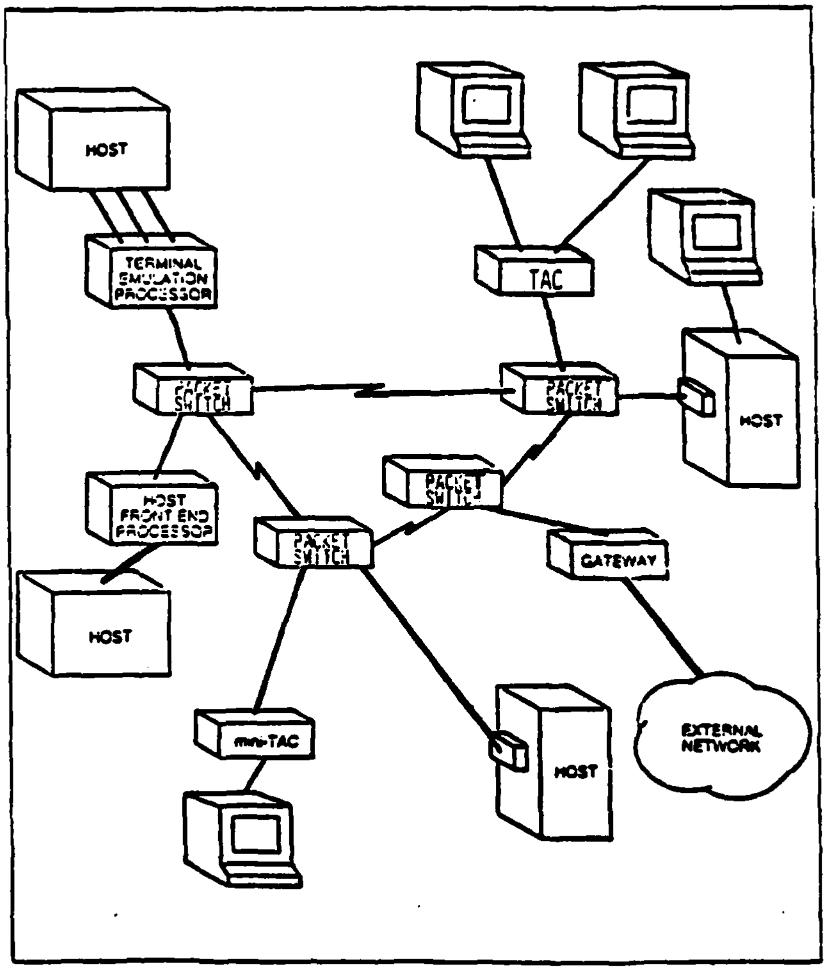


Figure 2.3 Simplified DDN Architecture

Source: Mitre Corp., 1984

following operating characteristics for asynchronous transmission:

1) Half or full duplex;

2) ASCII, BCD, or EBCDIC characters;

3) Choice of character format (i.e., number of stop bits and parity sense);

4) 5-9 bits per charaacter;

5) Optional flow control;

6) Externally clocked data rates;

7) Automatic terminal speed detecting;

8) In asynchronous mode, the TAC and mini-TAC provide for a maximum transmission rate of 9,600 bits per second (Mitre Corp., 1984).

Host computers will interface the DDN in a number of ways. Two common interfaces are the Host Front End Processor (HFEP) or the Terminal Emulation Processor (TEP). The HFEP provides high-speed synchronous serial ports to one or two hosts with the following operating characteristics:

1) Two-way simultaneous operation (full duplex);

2) 4,800 - 56,000 bits per second;

3) Transmits and receives binary data (Mitre Corp., 1984).

The TEP will support up to 16 ports for host system terminal connections on the subscriber side and up to two ports on the network side. The TEP can support asynchronous or synchronous transmission with operating characteristics similar to a mini - TAC. A host can also characteristics similar to a mini - TAC. A host can also access the DDN directly using the DDN X.25 interface protocol.

Monitoring Centers (MC's) are BBN C/70 processors running network software packages using the BBN UNIX-based operating system. The MC's main functions are to receive data from IMP's, TAC's and NAC's in order to monitor network status, configuration and performance (DDN System description, 1984). Specifically, MC's will monitor the status of network components, measure network performance, provide fault isolation and diagnosis, maintain network configuration data, support system test and evaluation and support packed switch software maintenance.

The original design for end-to-end encryption called for the use of Internet Private Line Interfaces (IPLI's) but these interfaces will no longer be part of the DDN. New Blacker technology presently being developed will supply the end-to-end encryption requirements of the DDN.

2.3 Network Criteria

The DDN needs to support some fundamental requirements that a user might have, especially when a user has to internetwork between two separate networks. Also, to use the network effectively, a user should implement specific network criteria. In order to accomplish these objectives from a user and network standpoint, specific requirements have been adopted for use in the DDN. The requirements have been adopted for use in the DDN. The following is a list that describes some network criteria that will provide:

1) for interoperability among heterogeneous devices. In order to accomplish this goal, specific computer protocols are required to be implemented in the networks involved with the DDN (specific protocols will be addressed later);
2) for low-risk technology so that the probability of failure of the system or the inability to be interoperable is kept to a minimum. ARPANET technology was chosen over AUTODIN II technology since it is proven technology;
3) for multi-level secure data communications. New BLACKER technology will provide the required end-to-end encryption and the integration of all segments of the DDN;
4) for reliable data transmission. Specific ARPANET protocols aid in the reliability of the communications. The expected undetected error rate is 4.2×10^{-18} or less using the

Transmission Control Protocol (TCP) and the Internet Protocol (IP). This, of course, is for continued optimal conditions. In reality, equipment failures due to catastrophic failure or battle damage will never allow this figure to be reached;

5) for expandability. The requirement for expandability is two-fold. First, it means that as technology changes, the network should change to meet those technological advancements; and second, that it be able to support increased users as the network expands. Modularity in design features will help ensure this;

6) for precedence and preemption. Many high-level users must have immediate communication ability; therefore, the system contains precedence message handling to allow a high-level of availability. The system must be available to a wide variety of users all the time. To accomplish this both a dynamic adoptive routing algorithm and virtual circuit concepts are used. The DDN provides 99 percent user-to-user availability to single-circuit users and 99.95 percent to dual-circuit users;

7) for DDN standardized components. This is done by requiring the users of the DDN to acquire

subsystems that can interoperate among host computers of the various other subsystems on the DDN. DDN x .25, APRANET protocols (TCP/IP), and specific application protocols accomplish this end;

8) for flexibility. The network should be able to tolerate changes in routing in order to meet user needs. Dynamic routing helps meet this requirement along with DDN gates that allow classified data to flow into the unclassified segment and then back into the classified segment. However, the reverse operation is not possible due to security reasons;

9) for survivability. This is accomplished by the system through the following variety of requirements:

   a) Redundancy - A large number of switches and multipaths are used;

   b) Dispersion - Packet switches are dispersed over the DDN system and located, when possible, away from high probability targets;

   c) Hardening - Some switches are located with users and, therefore, are hardened to the same degree as the user;

   d) Reconstitution - Includes transportable reconstitution nodes that can perform packet switching and monitoring;

e) Dynamically Adaptive Routing - Routes traffic around failed or congested switches.

That concludes the the discussion on the design and functions of the DDN. The next chapter consists of four sections and concludes with a comparative study between DDN X.25 and CCITT X.25. Before the actual comparison is made, a functional description of DDN X.25 is presented. Since there are three layers within the protocol, a separate section is devoted to each layer. The last section is the actual comparison between the two protocols.

CHAPTER III

DDN X.25 OVERVIEW

The purpose of DDN X.25 is to provide for the interfacing of DTE and DCE. DDN X.25 is based on CCITT X.25. The CCITT published its first X.25 protocol in 1977. The CCITT Recommendation used in this thesis was revised by Study Group VII during the study period from 1981-1984. This Recommendation was submitted to the VIIth Plenary Assembly at Malaga - Torremolinos, Spain in 1984. Therefore, DDN X .25 is composed of three layers as is CCITT X.25: the physical layer, the link layer, and the packet layer. Each layer has a specific function, and a number of options within those functions. Because CCITT X.25 does offer a number of options to its users, these options must be the same in specific networks, otherwise; the networks will not be interoperable.

Most of the DDN X.25 options are outlined in a federal standard. This standard was published in 1983 as a joint Federal Information Processing Standard (FIPS) and Federal Telecommunication Standard (FED-STD) by the combined efforts of the National Bureau of

Standards (NBS) and the National Communications System (NCS) (FIPS PUB 100/ FED-STD 1041, 1983). This Standard is the Federal Information Processing Standards Publication 100, Federal Standard 1041 (1983) and it "specifies the means of interfacing automated data processing (ADP) equipment and services, as well as telecommunication system terminal equipment, with packet-switch data communication networks. It is based on Recommendation X.25 . . ." (FIPS Pub 100, 1983, p. ii). FIBS Pub 100 defines the general requirements and options when implementing CCITT Recommendation X.25. The Defense Data Network X.25 Host Interface Specification by BBN (1983) further defines requirements and options when implementing X.25 in the DDN. Some specific requirements and options will be addressed separately.

For the DDN X.25 protocol to be interoperable with older interface protocols, two versions of DDN X.25 were developed. These versions were DDN Standard X.25 and DDN Basic X.25. DDN Standard X.25 is interoperable with the old interface standard Bolt Beranek and Newman (BBN) 1822 and any X.25 interface. DDN Basic X.25 provides communication only to other X.25 interfaces and not to BBN 1822. The key goal of the Government for using DDN X.25 as an interface is to have complete interoperability among all DDN subscribers. The use of

Standard or Basic is determined at the time of the call set up; therefore, it is done on a call-by-call basis (Mitre Corp., 1983).

Using DDN X.25 does not ensure true interoperability since upper layer protocols must also be implemented. For packet routing in the subnetwork, datagram protocols TCP and IP (TCP/IP) must be used. In addition, Application Programs should be used that employ one of the following protocols:

1) Telnet Protocol (character-oriented terminal support) provides communications between terminals and remote hosts (Telnet Protocol, 1984).
2) File Transfer Protocol transfers files in the network (Mitre Corp., 1984).
3) Simple Mail Transfer Protocol reliably and efficiently transfers electronic mail (Simple Mail Transfer Protocol, 1984).

All of the above protocols use TCP/IP at the lower level. One additional support function at the upper level is native mode. This is a software function that allows terminals and host of the same type to communicate.

3.1 Physical Layer

The physical layer has the responsibility of getting data from one point to another using some form of transmission media. Usually from a DTE to DCE, a hard-wire connection is made.

Layer one must accomplish a number of specific functions. It must determine the voltage level of the bits or signals being transmitted, the length of those bits, the type of transmission (i.e., asynchronous or synchronous), the initial connection and disconnection between the DTE and DCE, and finally how many pins are used by a particular connector and what signal characteristics each pin has (Tanenbaum, 1981).

In order for actual data to be transported from one DTE to another, a form of handshaking must take place, especially through the DTE/DCE interface. This is accomplished by assigning a particular function to a specific pin on the interface plugs being used. Changes of state on the pins signify changes within the DTE or DCE. One form of handshaking, call set-up, has a logical sequence of events. That is the DTE or DCE will receive a particular response for a given command it has sent.

All the transfer of data or signals takes place using various pin assignments by the particular interface being used. The DDN can use four different physical connectors. They are the Electronic Industries Association (EIA) Standard RS-232-C, the EIA STD RS-449, balanced and unbalanced, the military equivalent to EIA

RS-449, MIL-188-114, and the CCITT Recommendation V.35.

Tables 3.1 through 3.4 give a basic description of each interface and outline some of their principal operation characteristics.

Overall, the DDN performance or long-term goal is to use MIL-188-114B, the balanced interface, as the primary interface. The DDN cannot presently implement this requirement due to a limited amount of available vendor hardware (Mitre Corp., 1983).

3.2 Data Link Layer

The function or responsibility of the data link layer is to achieve reliable, efficient communication between an Interface Message Processor (IMP) and another IMP or between an IMP and a host computer (Tanenbaum, 1981:136). In the DDN X.25 interface protocol, the relationship will be between a host and IMP. The IMP to IMP protocol is different within the subnet of the DDN and will be covered later. Layer two must be able to take the raw transmission data and transform it into error free data with recognized frame boundaries, and then pass that data to the next layer. It also must take data from an upper layer and break the data up into frames, transmitting the frames sequentially and processing any acknowledgments sent by a receiver (Tanenbaum, 1981). The data link level can use two

Table 3.1 EIA Standard RS-232

EIA STD RS-232 interface characteristics:

1) Serial binary data exchange;
2) Data rates up to 20k bit/s;
3) Synchronous and asynchronous systems;
4) Dedicated 2 or 4 wire, point-to-point and multipoint operation;
5) 25 pin connector[1].

[1] Specific pin number assignments and associated circuits can be found in EIA Standard RS-232-C Booklet, 1969.

Source: EIA Standard RS-232, 1969

Table 3.2 EIA Standard RS-449

EIA STD RS-449 interface characteristics:

1) Serial binary data interchange;

2) Using RS-422 will support balanced signal operation;

3) Using RS-423 will support unbalanced signal operation;

4) 20k bit/s with RS-422 or RS-423;

5) Above 20k bit/s with RS-422;

6) Synchronous and nonsynchronous systems;

7) 37 pin - 9 pin connection (9 pin not required on DDN) (DDN Subscriber Interface guide, 1983.)

8) Used on analog telecommunications networks.

Source: McNamara, 1982

Table 3.3 MIL-STD-188-114

MIL-STD-188-114 balanced and unbalanced interface characteristics:

1) Serial binary data interchange;

2) 20k bit/s [1];

3) Above 20k bit/s [2];

4) Synchronous and nonsynchronous systems;

[1] MIL-STD-188-114 unbalanced is equivelant to RS-449 with RS-423.

[2] MIL-STD-188-114 balanced is equivalent to RS-449 with RS-422.

Source: BBN Corp.,1985

Table 3.4 CCITT V.35

CCITT Standard V.35 interface characteristics:

1) Is a wide modem;

2) Has data transmission rates of 48k bit/s using 60-108K Hz group band circuits;

3) Full-duplex operation;

4) Preferred transmission rate of 48k bit/s;

5) Synchronous operation.

Source: CCITT V.35, 1981

methods to process its information. It can dedicate lines to a given call, sending packets over the same line, similar to telephone switching services. This method is called a virtual circuit; or it can send separate packets over different lines not dedicated. This is called a datagram circuit. The word datagram, although used in DOD terminology, is no longer used by the CCITT. Study Group VII is presently studing an alternative to the datagram circuit such as connectionless service. (T. DeHaas, personal communication, November 1985).

The DDN X.25 protocol uses a virtual circuit method from the host to the IMP. Therefore, the host sees the entire circuit (end-to-end) as a virtual circuit, even though the subnetwork uses datagram circuits. The method used in the DDN interface is taken from CCITT Recommendation X.25 link level, called High-level Data Link Control (HDLC) Link Access Procedures (LAPB). According to the DDN X.25 Host Interface Specification Guide (1983), "DDN X.25 link Interface Specification Guide by BBN (1983), "DDN X.25 link level procedures are as specified by Federal Information Processing Standards Publication (FIPS) 100/Fed. Std. 1041 and CCITT X.25". FIPS 100 goes on to give mandatory interface characteristics at the link level, each of which will be discussed separately. FIPS

100 does this because there are many options and alternatives offered by CCITT X.25 and therefore they want Federal user requirements standardized when connecting to packet-switched data communications networks (FIPS 100, 1983).

3.2.1 Frame Structure

In order for the data link layer to perform its various functions, frames are constructed from the data coming from the upper layers. Figure 3.1 shows the basic HDLC LAPB format. The format is broken up into the following fields which have been adopted by the DDN:

1) Flag sequence - All frames start and end with a flag. This flag consists of one 0, followed by six 1's and then one 0. The flag sequence denotes the frame boundaries.
2) Address field - This field is one octet (8 bits in length) and identifies the receiver of the frame being sent and the transmitter of that frame.
3) Control field - This field is also one octet in the DDN; an option does exist that can enlarge this frame to 2 octets called modulo 128, but the DDN does not support it (BBN, 1983);
4) Information field - This field is the data from the upper layer protocols and carries a large

FLAG	ADDRESS	CONTROL	INFO	FCS[1]	FLAG
F 8-bits 01111110	A 8-bits	C 8-bits	I N-bits	FCS 16-bits	F 8-bits 01111110

[1] FCS - Frame Check Sequence

Figure 3.1 High Level Data Link (HDLC) Frame

Source: CCITT X.25, 1984

amount of control and supervisory information from those layers, but layer two looks at this field as transparent data and transmits it, regardless of what is actually inside the field. The information field in the DDN has a maximum number of 8248 bits or a data packet of 1024 data octets (BBN, 1983).

5) Frame Check Sequence (FCS) - The FCS field ensures error-free transmission by determining if errors exist within the frame itself. The DDN supports up to a 16-bit sequence. Modulo 128 can use a 3-bit sequence (CCITT X.25, 1984).

3.2.2 Frame Functions

There are a number of specific functions performed at this layer. The important ones are addressing, control, and error detection and are covered separately.

Addressing: Frames are routed through the system using the address field. This field will either be coded in a command or response format. The command format contains the address that the frame should be sent to at this layer, and the response format contains the address of the DTE or DCE sending the frame. This field also identifies particular multilink terminals depending on the coding of the bits. These addresses only correspond to the local DTE/DCE interfaces and not distant addresses across the subnetwork. The distant address is buried in the information field at this layer.

Control: The control field has many functions; its major work is performed by using three different formats in this field. They are the information transfer format, the supervisory format, and the unnumbered format. The following is a terse overview of each format since many situations can be depicted in the above field. (CCITT X.25, Document AP VIII-58-E, June 1984 has a complete list of formats.)

1) The information format is a command field that tells a receiving DTE or DCE the number of frames sent and received by the sending DTE/DCE;
2) The supervisory format can send and receive information on whether or not a corresponding DTE or DCE's receiver is ready (RR or RNR) for information and whether or not it needs a frame retransmitted (REJ). The supervisory frame also lists the number of frames it has received;
3) The unnumbered format allows for determining whether or not the transmission will be modulo 8, asynchronous balanced or if it will be modulo 128 asynchronous balanced mode extended. As mentioned before, the DDN will only accept modulo 8. The unnumbered field will also send

information such as a disconnect just happened or a frame reject response (FRMR). The FRMR will tell which frame was rejected and why.

All of the control frames mentioned above have a poll/final (P/F) bit in them. The P/F bit also has a number of functions. This bit is used to determine if a command or response should be given by a DTE or DCE. Specifically, all information formats are poll frames (command frames), while all supervisory frames and unnumbered frames will contain a poll or final bit (CCITT X.25, 1984).

Error Detection: The frame check sequence field is capable of determining if the bits that have been transmitted are correct or if a noisy link has caused an error. It checks bits existing between but not including the last bit of the first flag to the first bit of the FCS (CCITT X.25, 1984).

3.2.3 Frame Options and Parameters

There are a number of parameters and options specified by DDN X.25 that should also be discussed at this layer. The following list includes four major parameters and options:

1) There are seven frames (K) that can be transmitted through a DTE/DCE interface before an acknowledgment by the corresponding DCE or DTE

must be given. This window is called modulo 8. Modulo 8 at the link level has been stipulated by FIPS 100 (1983);

2) Timers ensure frames do not get lost along the interface. Only the transmitting and receiving timers will be discussed. (There are other timers but only three major ones will be covered;)

   a) Timer T1 - This timer is used by a transmitter to retransmit a frame that has not been acknowledged as received by a DTE or DCE (CCITT X.25, 1984). In DDN X.25, the T1 timer has been set at 4 seconds for the DCE for link speeds of 9.6k bit/s, and not lower then 3 seconds for speeds greater than 9.6k bit/s (BBN, 1983);

   b) Timer T2 - This timer is in the receiver and tells the receiver how much time is left after receipt of a frame in order to send an acknowledgment for that frame. The T2 timer will always be set less than the T1 timer (CCITT X.25, 1984);

   c) Timer T3 - If the channel remains idle too long after set-up, then this timer sends information to the upper layer to initiate another link set-up (CCITT X.25 1984).

3) A maximum number of attempts will be taken to complete a transmission (N2) - Normally the maximum transmission and retransmission of a frame after the timer has run out is 20 times, but this value can be as high as 200 times if need be (BBN, 1983).

4) The information frame (I) has a maximum length. In the DDN the length is held to 8216 bits or 1027 data octets (BBN, 1983).

This finishes the section on layer two the Data Link Layer. The next section covers the Packet Layer.

3.3 PACKET LAYER

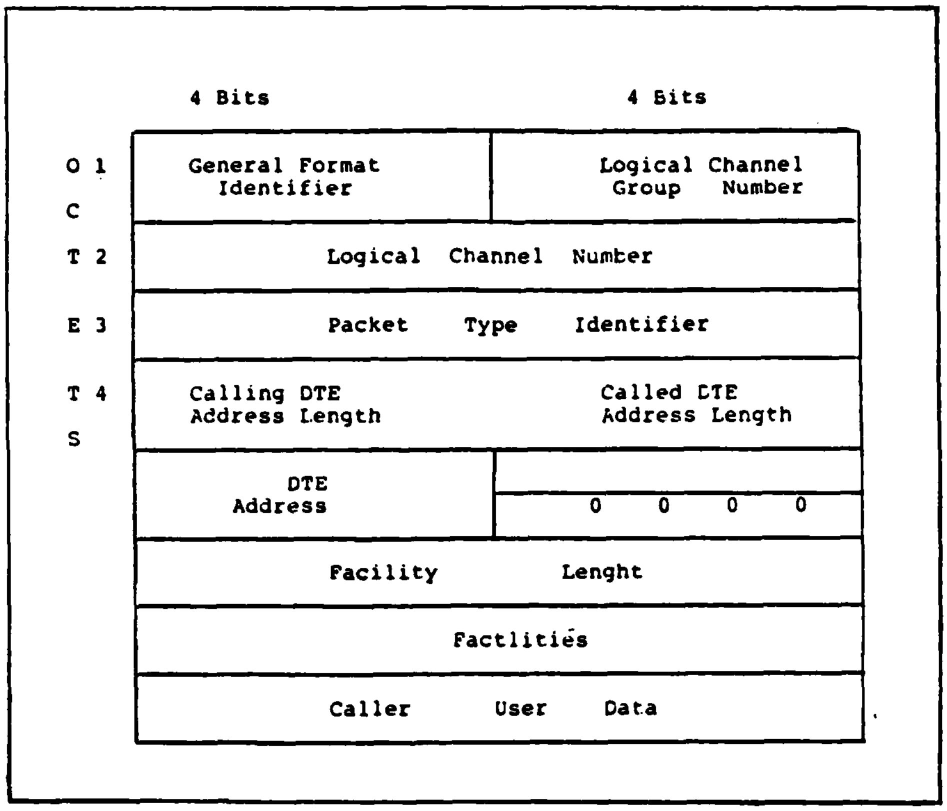
This layer, called the Packet Layer in CCITT Recommendation X.25, is also called the Network Layer and determines the fundamental characteristics of the host to IMP interface. It normally determines the routing within the subnet but in the DDN it will only be used as a host to IMP interface which creates some specific problems associated with a virtual circuit connected to a connectionless circuit such as the DDN. DDN subnet routing is done using the Internet Protocol (IP) discussed later. This section covers the X.25 interface HDLC protocol.

The HDLC LAPB protocol provides a virtual circuit between the DTE to DCE interface. Information in this layer is transparent in the link layer of the information field of the HDLC frame. As with the rest of the layers, there are many options available when implementing this layer. Using the basic CCITT X.25 standard, the Federal Government narrowed some of those options in FIPS 100 (1983). Finally, the DDN interface guide gives even more specific information on what the characteristics of that level should be.

The fundamental characteristics of this layer are discussed in the following paragraphs, along with problems associated with the layer.

3.3.1. Virtual Circuit Characteristics

The packet layer will allow for virtual calls and permanent virtual circuits. Virtual circuits are set up so that the information that is received remains in the order sent. Also, the virtual circuit is a connection that is made during the initial call set up procedure. That is, packet addressing remains constant for that particular call; therefore, only the initial packets carry the destination address. Packets are then transmitted sequentially through the existing virtual circuit. One format used at this layer is the call request and incoming call packet. This packet is shown in Figure 3.2. This particular packet requests a call set up between a DTE and a DCE. An interesting problem in



	4 Bits	4 Bits
O 1	General Format Identifier	Logical Channel Group Number
C		
T 2	Logical Channel Number	
E 3	Packet Type Identifier	
T 4	Calling DTE Address Length	Called DTE Address Length
S		
	DTE Address	0 0 0 0
	Facility Lenght	
	Factlities	
	Caller User Data	

Figure 3.2 Call Request Packet

Source: CCITT X.25,1984

the DDN is that the DDN uses virtual circuits until the packet gets to the IMP. Once in the internet, the DDN has a connectionless circuit using an Internet Protocol (IP). To solve this problem, the IP header carries the source and destination addresses, and the actual header is imbedded in the information field of the HDLC frame. Therefore, when the IMP receives the HDLC frame, it strips the frame out and leaves the IP header intact (M. Corrigan, personal communication, June 1985). In this way the system is converted from virtual circuit configuration to the DOD subnet protocols TCP/IP, a datagram configuration.

There are many types of octet packets depending on what type of control information is being transmitted (i.e. call request, call accepted, call connected, and clear request).

3.3.2 Packet Length

The data field length of an HDLC LAPB protocol is bit oriented, that is the information field can be of an odd or even number of bits to a given maximum length. This field does allow for data field lengths in an octet mode. The DDN presently has to support character oriented bits such as ASC II. In order for HDLC to be used, the information frame is made up of characters of specific lengths that are octet aligned. The DDN supports packet sizes of 16, 32, 64, 128, 256, 512 and 1024 octets (BBN, 1983).

3.3.3 Addressing

Embedded in the packet in Figure 3.2 are the called and calling DTE address. The DDN uses a format that is made up of four seperate fields. The first field is 4 bits in length and is reserved for future use; it is presently coded to zero. The next field is a one bit flag. This flag differentiates between a logical or physical address. A one is used to denote a logical address, a zero is used to denote a physical address. This third field is the DDN host identifier. It consists of seven digits and can be a physical or logical address. The final field is a two digit field called the sub-address and is an optional field that can be used by the DTE for any reason (DDN X.25 Interface 1983). This field can be up to 14 characters in length.

3.3.4 Call Set Up

Call set-up procedures are done using a call request packet from a DTE or an incoming call packet from a DCE. If the called DTE can accept a call, it will transmit a call accepted packet to its DCE. The calling DTE will then receive a call-connected packet. At this time, data transfer can take place since the logic states of the connector pins will be set to transmit or receive data (CCITT X.25, 1985). There are many other specific functions and formats that the DTE and DCE use to exchange control types of information (See CCITT X.25, Document AP VIII-58-E, June 1984, Sect. 4 for additional information).

3.3.5 Flow Control

Flow Control is accomplished by only allowing specific packets to go through the DCE/DTE interface. Before the packets are sent, they are sequentially numbered, then a window (W) is advanced as the packets are sent. If a packet number does not match the window number, it cannot be sent out. That means according to CCITT X.25, "The packet send sequence number of the first data packet not authorized to cross the interface is the value of the lower window edge plus W (modulo 8, or 128 when extended)" (CCITT X.25, 1985). When the first packet is sent, the value of the lower window edge becomes zero, and the present value of W is 2 for each direction of data flow across the DTE/DCE interface.

3.3.6. Precedence

Precedence levels are needed in the DDN to ensure that more important information can be transmitted through the network by interrupting lower precedence information. CCITT Recommendation X.25 does not deal with precedence levels, but does allow for options in the facility field of specific packets. These packets which have facility fields are the call request, incoming call, call accepted, call connected, clear request, clear indication or DCE clear confirmation packets (CCITT X.25, 1984). DDN X.25 uses this option to set up call precedence in the network. A two-octet field is used, and is coded in the following way: 00001000 000000XX. The XX represent the precedence level and can go from 00 (lowest precedence) to 11 (highest precedence) (BBN, 1983).

The DDN must interface this code with the IP protocol. Therefore, the IP header, type-of-service field code, must be mapped into DDN X.25. DDN X.25 does not support all precedence levels the IP type -of-service field supports. Table 3.5 shows the mapping and precedence levels supported by DDN X.25.

Of course, once in the subnet, all the IP precedence levels will emerge but at the local level only up to flash can be seen by the DDN X.25 interface.

3.3.7 Acknowledgments

In CCITT Recommendation X.25, there is a delivery

Table 3.5 Precedence Level Mapping

IP Precedence		DDN X.25 Precedence
000	Routine	00
001	Priority	01
010	Immidiate	10
011	Flash	11
100	Flash Override	11
101	CRITIC/ECP	11
110	Internetwork Control	11
111	Network Control	11

Source: BBN Corp., 1983

conformation bit (D bit) that can be used if the DTE wishes to receive an end-to-end acknowledgment of delivery. This bit is the seventh bit in the General Format Identifier of a call request packet. Setting this bit to one ensures the DTE of the end-to-end acknowledgment. The DDN does not use this capability since end-to-end conformation is done at layer four, the Transmission Control Protocol (TCP) layer (BBN, 1983).

3.3.8 Diagnostic Packets

Diagnostic packets are used to give information on any error conditions that exist within the network. Each packet contains a code with corresponding error conditions. CCITT X.25 lists over 65 codes. An example would be the code 01000011 which corresponds to an invalid called address. There is a total possibility of 255 codes words, but from the decimal number 128 to 255 there are no codes assigned and that space is reserved for network specific diagnostic information (CCITT X.25, 1984). The DDN uses these additional diagnostic codes for its own network. An example of this would be the decimal 194 code which means that a call has been cleared due to a higher precedence call at a remote DCE (BBN, 1983).

3.3.9 Fast Select Option

One more fundamental characteristic of this layer is the use of the Fast Select option. Fast Select is an option that can be exercised in a call set-up procedure by a DTE. The option shows up in the facility field (see Figure 3.2) and allows a call packet to contain a user data field of up to 128 octets. This option can be used in any of the following types of packets: the call request, call connected, clear indication, and/or clear request packet. The DCE can use what is called a Fast Select Acceptance. In this way, the DCE can send user data packets of 128 octets in length to the DTE. The following types of packets can be sent by the DCE: the incoming call, clear request, clear indication, and /or call connected (CCITT X.25, 1984).

FIPS PUB 100 (1983) states that a DTE calling the network does not have to subscribe to fast select but must be able to accept incoming fast select packets.

The key to this layer is its ability to be interoperable with the Internet Protocol (IP) layer. In order for this concept to work, IP datagrams are imbedded in DDN X.25. DDN X.25 is only used at the local layer where IP is used within the subnetwork. The IP layer will be covered in the next chapter when the DOD Protocol Reference Model will be discussed.

3.4 Comparative Study Between DDN X.25 and CCITT X.25

The use of CCITT X.25 is mandated by the Federal Government through the Federal Information Processing Standards (FIPS) Publication 100, Federal Standard 1041; therefore, the basic fundamental principles of CCITT X.25 were already covered under DDN X.25. The differences lie in the options and alternatives used by the DDN which were also already covered in this chapter. It should be noted that the CCITT X.25 Recommendation used as a reference in this thesis is newer than the CCITT X.25 reference used by Fed. Std. 1041. The major difference being that the newer version has enhanced services that are provided to the user. Some of these differences include :

1) Changes like the Fast Select option is now an essential capability;
2) Up to 32 bits of expedited data can now be carried in an interrupt packet versus the former recommended packet;
3) There are five new DTE optional facilities that support end-to-end signaling. These new options will bring X.25 into full compliance with the OSI Network Layer Service Definition (Ingram, 1985).

Even with these changes CCITT X.25, 1984, is upwardly compatible with CCITT X.25, 1980 and therefore, use of the 1984 version will allow interoperability with the 1980 version. FIBS PUB 100 will reflect the use of the 1984 Recommendation during its next version (W. Ingram personal communication October 8, 1984). (For a complete description of differences, see a draft analysis done by William Ingram, NTIA/ITS Boulder, Colorado.)

Although DDN X.25 is not exactly like CCITT X.25 because of the options and alternatives, the basic structure of X.25 remains and minor changes in the software design can allow for these additional changes.

To ensure that manufacturers have met DDN specifications, the Defense Communications Engineering Center (DCEC) has established a testing procedure. This testing procedure was develcped by the Institute for Computer Sciences and Technology (ICST) of the National Bureau of Standards (NBS) and the National Communications System (NCS) (Clark, 1985). To ensure the testing procedure used by DCEC is accurate, use is made of a chameleon protocol tester by Tekelec (Clark, 1985). This tester ensures that a device under test has correctly implemented the specifications of X.25 for use in federal automated data processing equipment (ADP). The tests are based on test sequences derived from CCITT X.25 specifications using state matrics. "The rationale for using these matrics is that they identify all permissible states and conditions relevant to the correct execution of any X.25 implementation" (Clark, 1985:154).

The Federal Government, by using an internationally accepted protocol, has been able to implement a number of important ideas. These four ideas of adapting to new technology, maintaining and supporting present systems, decreasing system costs, and interlinking separate systems are outlined in the following paragraphs.

First, networks should become more adaptable to changes in technology as that technology becomes available. By mandating the use of an international standard in a government standard, the government can take advantage of these changing technologies as they are implemented in international standards. This will lead to a quicker transition to newer protocol designs. Standards organizations do take time to adopt to a new technology, but once the standard is adopted, it becomes accepted by a wide variety of users, and as enhancements come about there is even less time to have them accepted and, more importantly, implemented. Along with this idea is the concern of international standards organizations that the standards process needs to be speeded up. Cerni (1894) mentions the fact that international organizations such as International Electrotechnical Commission (IEC), ISO, and the CCITT are trying to work more closely to decrease the time it takes to develop a standard. This factor enhances the Government's and DOD's need to adopt international standards whenever possible.

Next, the network can become more supportable and maintainable. This is because many manufacturers are increasing their support for international standards. In fact, there has been an explosion of standards setting in the last decade and a half, during which time 70 percent of all international standards have been created since 1970 (Cerni, 1984). This has led to more and more off-the-shelf designs that have incorporated international standards, allowing more vendors to supply products that reflect these new standards. There is a two-fold advantage to this in that not only is more equipment available but also that it is offered by a wide variety of manufacturers.

This third idea of affordability is seen when the DOD uses off-the-shelf vendor equipment rather than specific DOD designed equipment. One study done by the Defense Communications Agency (DCA) is a good example of how the DOD could have potential savings using commercially vended software (WWMCCS-ADP). Also, Donald C. Latham, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, stated in his reply to an NRC Report (Postel, 1985) that "Whenever international standards are available and can be used to support military requirements, they will be implemented as rapidly as possible to obtain maximun economic and interoperability benefits" (Postel, 1985, p. 2). These previously stated factors also allow for the equipment to become more affordable since added competition will tend to reduce the price of the product.

A final benefit and major goal of the Department of Defense is that networks should be interoperable. Of course, a requirement of interoperability is that the networks must use the same interface protocols. Access to the DDN using DDN X.25 in all DTE to DCE interfaces fulfills this requirement. Also by using an international standard, more North American Treaty Organization (NATO) networks will, in fact, be interoperable. This idea of interoperability has become a key study factor for the NATO Advanced Study Institute on Interlinking of Computer Networks (Beauchamp, 1979). One study by the Institute shows that PTT's are adopting Recommendation X.25 as an interface for packet-switched networks (Beauchamp, 1979).

It becomes obvious that a DOD conformance to an international standard can derive many benefits that would otherwise be unavailable. Most importantly are the benefits of access to new technological developments and the increased capability of interoperability through standardization. The alternative is for the DOD to have specialized technological development take place within their networks that no other system is going to use and then having to support and maintain such a network through long procurement cycles and costly maintainance requirements. Again, the issue of interoperability becomes paramount because if no other forces, national or international, have aligned their networks with the DOD's, then the DOD can suffer from owning and operating unique equipment that cannot interlink with these forces in times of international conflict.

CHAPTER IV

INTERNETWORK AND TRANSPORT PROTOCOLS

To establish a comparison between the protocols used in the DDN and industry, the characteristics of the networks will be viewed from the perspective of layered reference models. Three different DOD Protocol Reference Models have been selected in this thesis and compared to the ISO Open System Interconnection (OSI) Reference Model. Figures 4.1 and 4.2 show the comparison of the different models.

There is some ambiguity as to where to align the layers of the DOD model with the layers of the OSI model. Therefore, a determination is made on how to treat the ambiguities. That is, regardless of which model is used a specific point is taken within that model and a definition of its characteristics stated. This leads to a specific layer in each model, depending on the author's view of which layer fills those specific characteristics. The following paragraph explains how this concept is used in this thesis.

Chapter three defined the interface into the DDN. This interface represents a virtual circuit from the DCE

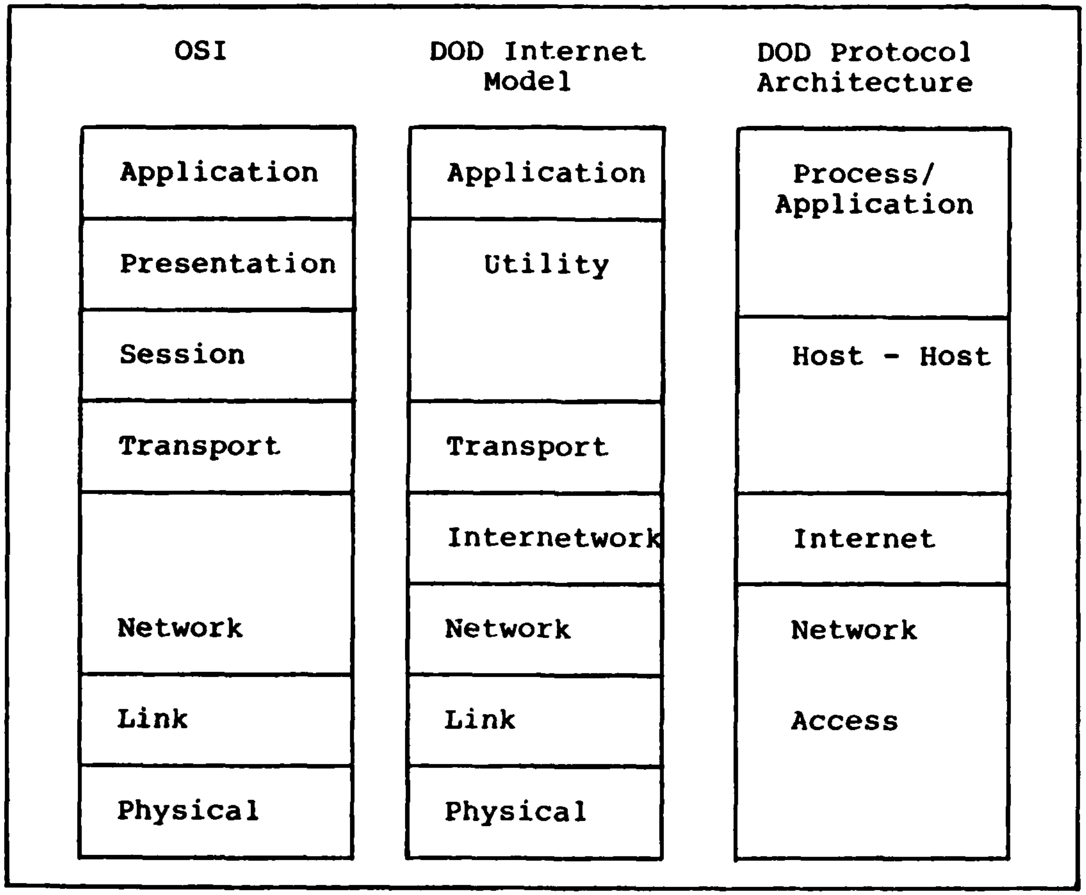
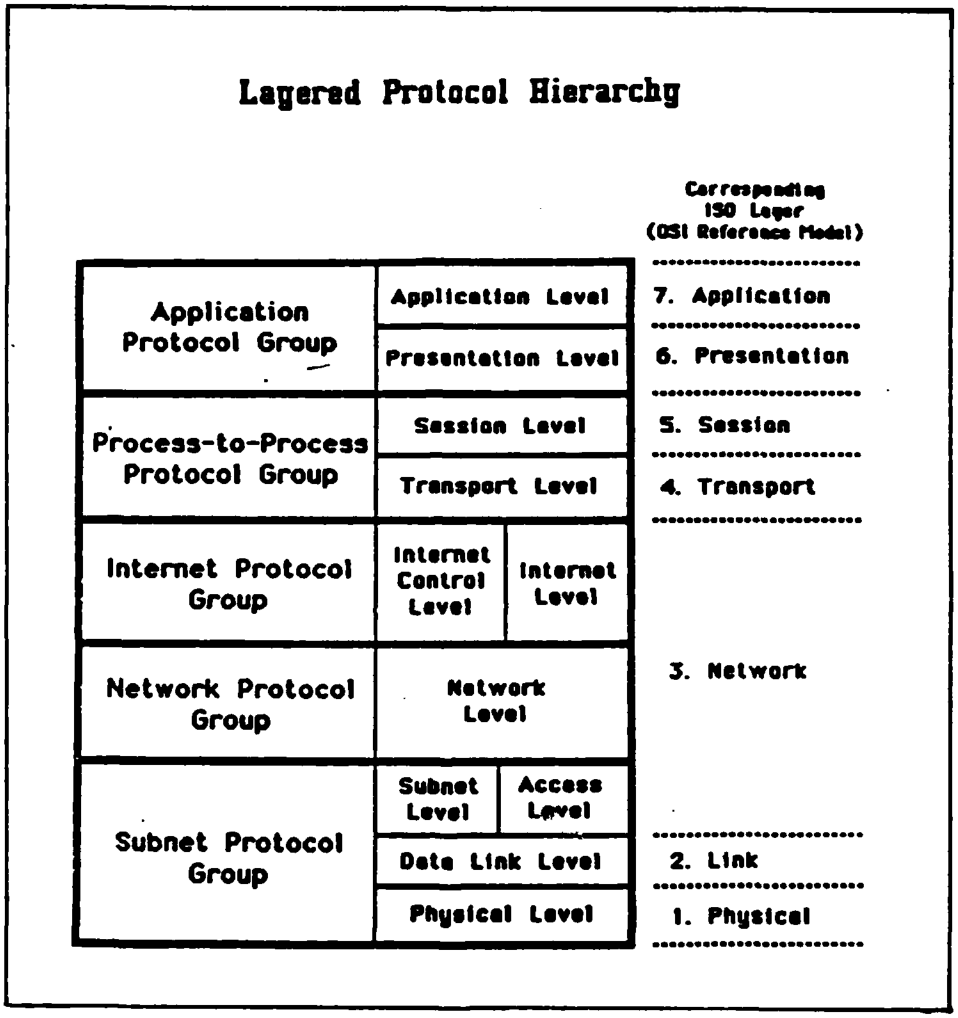


Figure 4.1 DOD Comparative Models

Sources: OSI - Tanenbaum, 1981
DOD Internet - Cerf, 1983
DOD Protocol - Stallings, 1985b



Layered Protocol Hierarchy

		Corresponding ISO Layer (OSI Reference Model)
Application Protocol Group	Application Level	7. Application
	Presentation Level	6. Presentation
Process-to-Process Protocol Group	Session Level	5. Session
	Transport Level	4. Transport
Internet Protocol Group	Internet Control Level Internet Level	3. Network
Network Protocol Group	Network Level	
Subnet Protocol Group	Subnet Level Access Level	
	Data Link Level	2. Link
	Physical Level	1. Physical

Figure 4.2 DOD Comparative Models

Source: Air Force Information Systems Architecture, 1985 to DTE interface that is equivalent up to the network layer of the OSI model. Once inside the subnetwork, the DDN uses a protocol that transmits datagrams (packets) from a source Interface Message Processor (IMP) to a destination IMP. This protocol, by using the above concepts, is also considered in the communication subnet layer or network layer within the OSI model. The source IMP to destination IMP protocol is known as the DOD's Internet Protocol (IP) and is discussed in this study. The industry protocol used for this comparison is taken from an ISO draft international standard (DIS 8473). The draft standard is in its final stage of approval, having passed the draft international standard (DIS) ballot (D. Walters, personal communication, November, 1985). This protocol is actually a sub-network protocol called the Connectionless-mode Network Protocol (CLNP).

IP is also used in conjunction with the DOD's host-to-host protocol, called the Transmission Control Protocol (TCP). Since TCP is an end-to-end protocol, it equates to the transport layer protocols of the OSI model; therefore, a transport layer from the OSI model is the industrial comparison in this study. The approach used to define the DOD layers in reference to the OSI layers will help to alleviate any ambiguity between the reference models.

In the comparative study, the analysis of IP and

TCP will be covered in more depth than the ISO protocols because of their complexity.

4.1 Internet Protocol (IP)

The Internet Protocol (IP) performs two basic functions. It is a source-to-destination protocol within a network, and it acts as a gateway betweeen networks. IP provides datagram service from sources to destinations within the internet (Internet Protocol, 1983). This source to destination service is also provided by the network layer of the OSI model (Tanenbaum, 1981). Therefore, using the data flow from source to destination IMP's as a point of reference, clarifies that protocols from the network layer of the OSI model can be compared to protocols from the DOD's Internet layer.

IP also functions within the internet (or subnetwork) and is designed to interconnect other packet switched subnetworks to form an internetwork (Internet Protocol, 1983). The IP layer must provide specific services to the upper layer protocols (ULP) and receive specific services from the lower layer protocols (LLP) in order to function properly. As discussed in Chapter 2 of this thesis, the IP layer and all other ULP's are embedded in the information field of an HDLC LAPB frame. The source IMP strips out the HDLC frame and sends the packet on its way, while the destination IMP will deliver a datagram with an IP header to a receiving DCE for HDLC framing.

4.1.1 IP Structure

A basic IP header is shown in Figure 4.3. A brief description of each field follows:

1) Version - This indicates the format of the IP header. This header is version 4;
2) Internet Header Length (IHL) - This is the length of the IP header and it also points to the beginning of the data. Each bit represents a 32-bit work sequence on 4-octet groups;
3) Type of Service - This field contains the IP parameters describing the quality of services for the datagram. Precedence is imbedded in this field along with delay, throughput, and reliability bits;
4) Total Length - This is the actual length of the datagram to include the data field and header;
5) Identification - If a datagram has been fragmented, this field will allow for association of those fragments;
6) Flags - This allows an ULP to request that a datagram not be fragmented. It also is used to tell if more fragments are coming or if it is the last fragment;

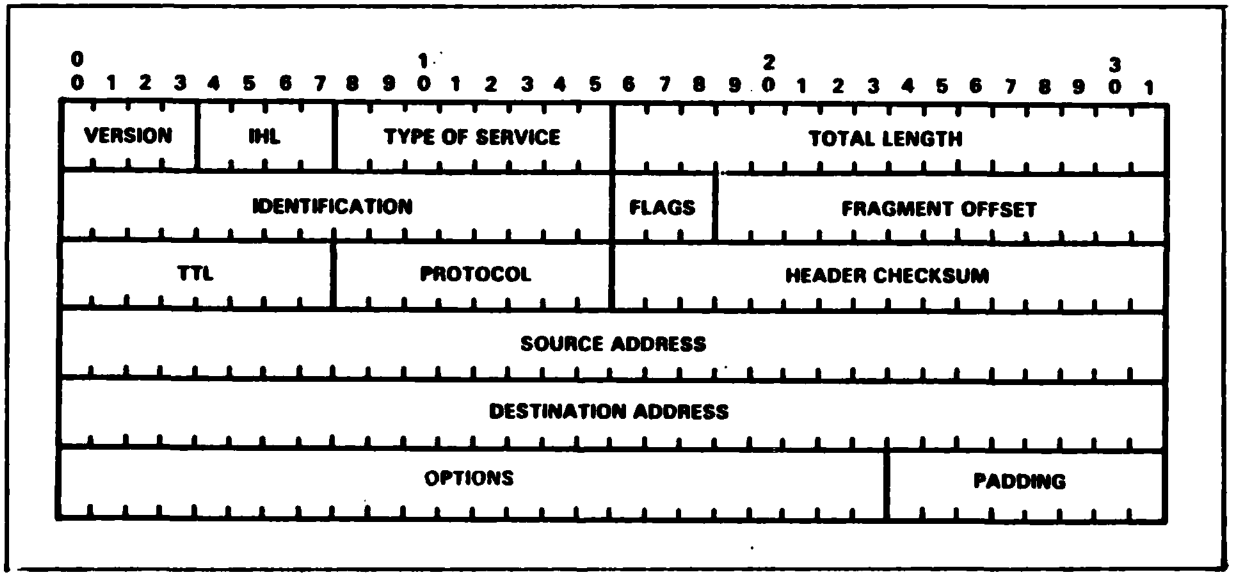


Figure 4.3 Internet Protocol Header

Source: Internet Protocol, 1983

7) Fragment Offset - This field indicates the relative position of the data in the datagram to the data in the original unfragmented datagram;

8) Time-to-live - A datagram is given a specific amount of time it can be routed within the system. When the field reaches 0, the datagram is discarded;

9) Protocol - This field indicates which ULP will be receiving the data from the IP;

10) Header checksum - This field checksums the header;

11) Source address - The internet address of the source host is in this field;

12) Destination address - The internet address of the destination host is in this field;

13) Option - There are a number of options which can be employed in this field. They will be covered later in the text;

14) Padding - The padding field ensures that the header remains in an octet format; therefore, it ensures a 32 bit boundary (Internet Protocol, 1983).

IP has no control over certain functions such as flow control or error control on the data portion of the message. IP datagrams also do not have acknowledgments (Stallings, 1985). These functions are part of the upper layer protocol already mentioned called TCP. It is the TCP/IP relationships that enable the DDN to have an internetworking capability that is robust and error free. The main function of IP is to deliver a packet to the destination host whether that host is in the same network or some other network.

4.1.2 IP Characteristics

There are a number of characteristics needed within IP before it can accomplish the simple task of delivering the packet. Six of these characteristics described below are: addressing, routing, fragmentation and reassembly, time-to-live, type of service, and options.

Addressing: There is a four octet (32 bit) length address. It is broken up into a network address followed by a local address. Figure 4.4 shows four classes of addresses used in the datagram: classes a,b,c, and an extended undefined address field (Internet Protocol, 1983). The a, b, and c classes give a variety of addresssing formats for the network and local addresses, allowing for addressing of a large number of small to medium networks. The last class has no specific format

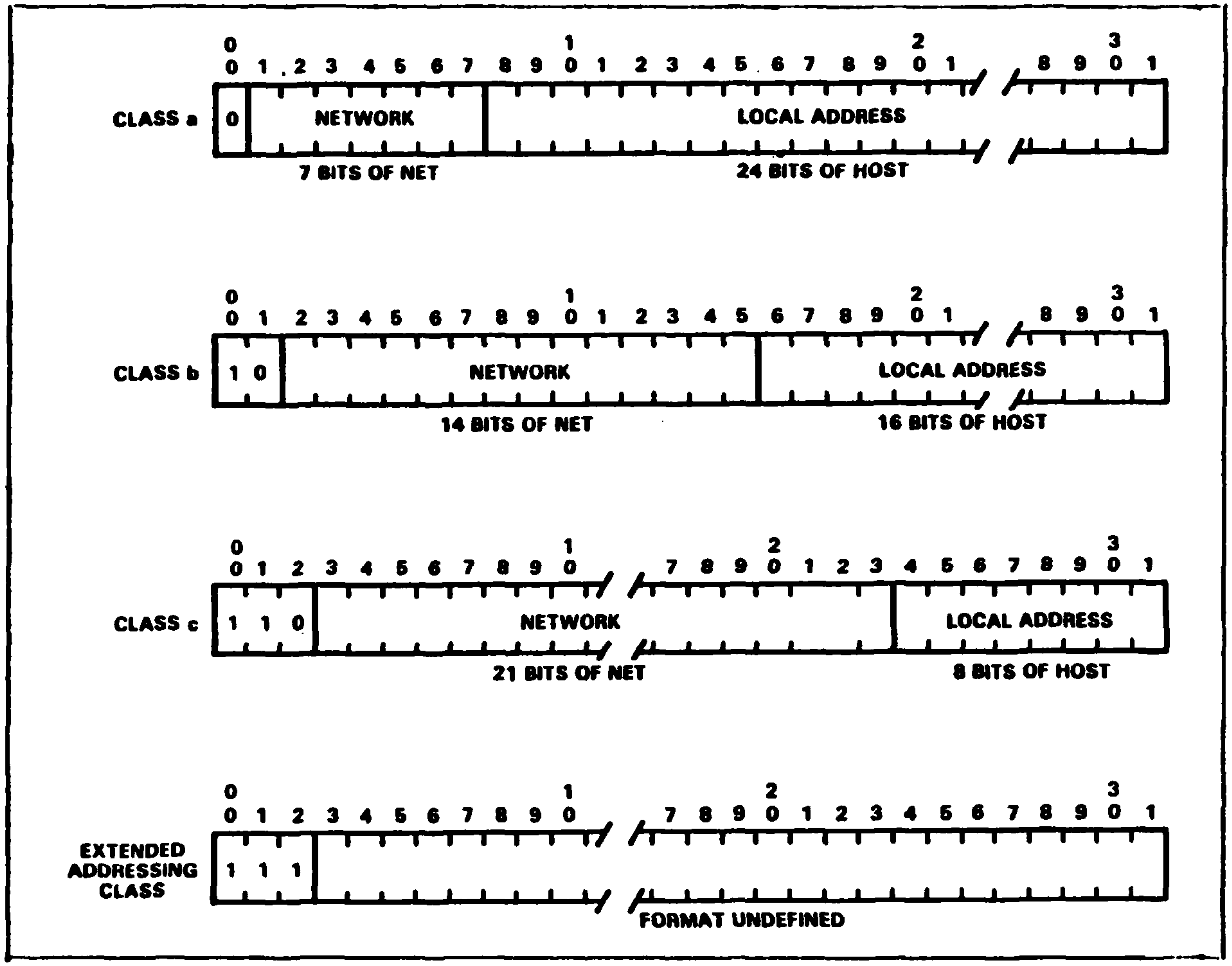


Figure 4.4 Internet Addresses

Source: Internet Protocol, 1983

except in the first three bits which are used to identify which class is being used. IP hardware equipment (module) examines the network address to determine if the datagram belongs in that network; if so, it then looks at the local address and determines to which host in its subnetwork the datagram should go. If the network address is different, then the IP module must determine how to route the datagram. The IP module will then use its current dynamic routing table to determine the path (Internet Protocol, 1983).

The source and destination addresses allow the IP module to deliver an IP datagram within the subnet from one host to another through each IMP. A problem arises when the datagram must be delivered to a different subnet across a gateway. In order for the proper addressing scheme to take place, a local subnetwork protocol (SNP) is invoked. The local subnet protocol hardware builds an additional header in front of the IP header. The SNP takes the local subnetwork address (a gateway address) from the IP module and creates the header in front of the IP header that will route the datagram through the local subnetwork to the gateway. At the gateway, the SNP is stripped out and the IP module within the gateway then determines from the internet address which subnet to go to next. The SNP protocol is used again until the datagram reaches the proper subnetwork, then the destination SNP strips out the SNP header and passes the datagram to the destination IP module. The IP module of the proper subnetwork sends the datagram to the host (Internet Protocol, 1983).

Routing: An IP module must determine how to route a datagram through its network or into another network. Either way, the IP module must concern itself with what route to use because of network or gateway failure or because of long queuing times. In order to alleviate these problems, IP modules exchange dynamic routing tables. These tables are updated periodically between IMP's and contain information on errors, congestion and/or equipment failures within the network and gateways. The tables also give information on the number of hops to the destination and the next gateway on the route (Stallings, 1985a). The tables maintain the updated topology of the networks involved, and along with the other information, an IP module can use loose or strict source routing of its datagrams (Internet Protocol, 1983). In loose routing, the IP module can take any number of intermediate gateways to reach the source. Strict routing is a directed route from an ULP. The ULP provides a source routing list that the IP module must use. This list determines the route the datagram must take. If the route cannot be taken, an error condition occurs and the IP module sends an error message to the source host (Internet Protocol, 1983). These routing conditions are part of the "options" format in the IP header.

IP also receives gateway routing help from a Gateway-to-Gateway protocol (GGP). GGP helps "determine connectivity to both networks and neighbor gateways, and to implement a dynamic, shortest path routing algorithm" (Hinden, 1983, p. 231).

The GGP probes other gateways and other network interfaces. These probes require responses and if no response is received then the gateway or network is considered down (Hinden, 1983). The GGP uses this information to update its routing table and transmits these tables to other neighbor gateway addresses. In this way, dynamic routing tables are constantly being reconfigured.

Fragmentation and reassembly: Datagrams that traverse subnetworks must be able to meet the size requirement of different networks. IP provides services that allow for fragmentation of a large datagram if required. As the fragmentation takes place, the data is broken down into a minimum size of eight octets (Internet Protocol, 1983). Of course, the IP header contains information on the relative position of the data within the fragmentation as compared to the original unfragmented datagram. In order to accomplish fragmentation and reassembly, the IP header uses the total length, identification, flag, and fragment offset fields of the IP header (Stallings, 1985a). (See previous description of IP header fields.) All fragmented datagrams are reassembled at the destination host IP layer (Internet Protocol, 1983). Since only the destination host reassembles the data, datagrams can become very small while moving through different networks. In fact, a datagram can have a header size of 60 octets while its data field is only eight octets (Internet Protocol, 1983). This can impair the efficiency of some networks because it introduces more traffic as the acceptable size becomes smaller. But reassembly at IP gateways would require large buffer space, and the requirement that each fragmented datagram use the same route through the networks (Stallings, 1985a).

Time-to-Live: In a datagram service that is connectionless, some parameters must be available so that the datagram does not loop around subnetworks inefficiently without getting to its destination. ULP's determine the number of maximum hops (passes through an IP module) that a datagram can take. Once the datagram has traversed its maximum number, the packet is discarded (Internet Protocol, 1983).

Type of service: An upper layer protocol can request a specific service from a lower layer protocol. IP provides four services to TCP. These services include a precedence level, a delay indication, a throughput indication, and a reliability indication (Internet Protocol, 1983). The precedence levels of IP were discussed in Chapter 3. The precedence level indicators are set using the first three bits of the type of service field. The last three services are more of a trade-off. These service parameters will help the IP to determine which network or route should be taken by the datagram (System Development Corp., 1982). Setting the delay parameter bit to one means the datagram should experience less queuing within the networks involved (Tanenbaum, 1981). Setting the reliability bit to high (one) establishes the fact that the datagram should traverse a network with a low time between mean failures and/or good line conditioning (System Development Corp., 1982). These two parameters already begin to have trade-off implications since getting less delay from the network could mean having to use a line with more noise. Finally, setting the high throughput indicator bit to one takes into account the information transfer capacity of the network (System Development Corp., 1982). Each ULP must determine what its requirements are and usually only two out of the three are set to one.

Options: There are six options available in this protocol

(Internet Protocol, 1983). One is the level of security that the datagram is carrying. This option enables the subnet to know whether it is allowed to pass the information through its network. Another two options allow for strict or loose source routing by the IP (covered in previous section on routing). The other three options are:

1) Record Route - This option records the route a datagram has taken. There is a maximum number of routes that can be recorded even if the datagram goes through more internet addresses before arriving at the destination;
2) Stream Identifier - This option supports the stream concept used in some DOD networks;
3) Internet Timestamp - As the datagram traverses the network, IP modules can timestamp the datagram. This is a 32 bit value of the current time in milliseconds since midnight Universal Time (UT) (Internet Protocol, 1983).

4.1.3 Internet Control Message Protocol

This protocol provides an additional service that helps control the internet. This is done by the use of another protocol called the Internet Control Message Protocol (ICMP). As with X.25, diagnostic packets are sent that give status of the network by the ICMP. Some of these messages are destination unreachable, time exceeded, parameter problems, and redirect (Stallings, 1985b). The information in the ICMP protocol is attached to an IP header before being transmitted (Stallings, 1985a).

As discussed before, the IP has no flow control mechanism or acknowledgment mechanism. Also, messages can be dropped because discarded error-lost-messages are not always accounted for using only IP. Therefore, a reliable end-to-end protocol must be incorporated. The DDN uses the DOD's Transmission Control Protocol (TCP) for these purposes. The next section discusses the characteristics of TCP.

4.2 Transmission Control Protocol

"TCP appears in the DOD protocol heirarchy at the transport layer" (Transmission Control Protocol, 1983). In viewing figure 4.1, it can be seen that all reference models put TCP at the transport layer of the OSI model. The key factor of this layer is that it uses end-to-end or host-to-host protocols and is the first layer to carry on a conversation from the source to destination (Tanenbaum, 1981). TCP is set up to provide a connection-oriented transfer of data that is reliable, ordered (in terms of the packet order), full-duplex, and flow controlled (Transmission Control Protocol, 1983). It is important to note that this layer is a virtual circuit layer that requires a call set up, data transfer, and connection-close handshaking procedure. The transport layer is the most complicated layer and is the "keystone" of the concept of computer-communication architecture (Stallings, 1985a). For this reason, the problems associated with this layer will be covered along with the methodology for solving those problems using TCP.

4.2.1 TCP Structure

Figure 4.5 gives the TCP header structure. A brief description of each field is covered below:

1) Source Port and Destination Port - These numbers are 16 bits each and identify the source and destination ports;

2) Sequence Number - The sequence number is a value which represents the first data octet of a segment;

3) Acknowledgment Number - These numbers are used to keep track of the sequence number the sender of a

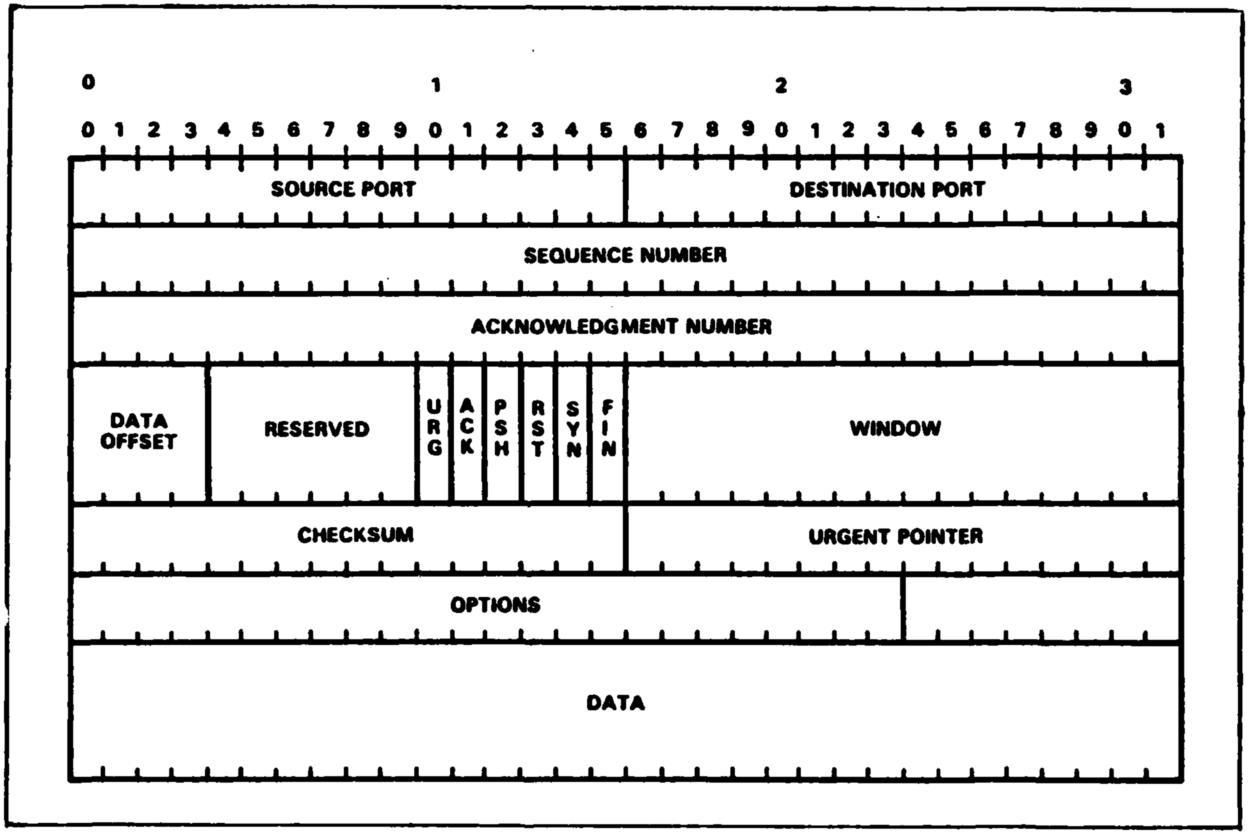


Figure 4. 5 Transmission Control Protocol Header

Source: Transmission Control Protocol, 1983 segment is expected to receive;

4) Data Offset - This field identifies where the actual data within the datagram begins;

5) Reserved Field - The field is as stated, reserved for future use;

6) Control Flags - The six control flags carry information used in the connection establishment, termination, and maintenance of a connection (each will be discussed separately);

7) Window - This field is a 2-bit field which has the number of data octets the receiver is willing to accept from the transmitter;

8) Checksum - The checksum field checks the header and text for transmission errors;

9) Urgent Pointer - The pointer is used to point to the sequence number of the octet following the urgent data;

10) Options - Three options are available using the TCP. They are an end of option list, a no-operation, and a maximum segment size;

11) Padding - Padding ensures that the 32 bit boundaries are adhered to, so that the TCP header ends and the data begins on a 32 bit boundary (Transmission Control Protocol, 1983).

The following section gives an analysis of the characteristics of TCP from a functional level. This section also discusses specific problems within this layer and how TCP deals with these problems.

4.2.2 TCP Characteristics

TCP works in conjunction with IP and has its own characteristics in order to accomplish its goal of delivering datagrams from host to host. Four major characteristics discussed in this section are: connection establishment and termination, positive acknowledgments with retransmission, flow control, and addressing.

Connection establishment and termination: An attempt to open a connection between two hosts at the transport level within the DDN is complicated by the fact that the lower layer protocol is a datagram service that is only required to deliver the datagram. Therefore, when connection establishments are being attempted, acknowledgments must be sent back to the sender to ensure that the receipt of a Request for a Connection (RFC) was received (Stalling, 1985a).

What complicates the issue is that RFC's can be delayed within the datagram internet causing a transmittter timer to time out and retransmit another RFC, causing two RFC's to arrive at the receiver. Also, receiver acknowledgment can be delayed causing two acknowledgments to be present. A worse case exists when a second RFC arrives after the initial has been terminated, thereby causing a new connection to be made. In order to deal with this problem, a sequence number is attached to a transmitted RFC. The receiver's acknowledgment of the RFC will contain that particular sequence number. This procedure continues through the entire exchange of data using successive sequence numbers. In this way, an old RFC with an incorrect sequence number will be rejected. TCP uses a Synchronize Sequence Number (SYN) instead of an RFC. The SYN flag is part of the control flag field within the TCP header (Transmission Control Protocol, 1983).

Connection termination begins when one side, side A, of the connection determines it will not send any more data. To accomplish this, TCP sets the No More Data From Sender (FIN) flag. The flag tells side B that no more data will be sent by A. After B receives this FIN, it sends an ACK along with its own FIN. If B has additional data, it can be transmitted with the ACK. Side A receives the data and the FIN and returns an ACK, then closes its side of the connection. Side B receives the final ACK and closes its side. Abrupt closes can take place because of preemption and/or equipment failure.

These closures usually result in a loss of data between the two sides.

Positive acknowledgments with retransmission (PAR): Another area of concern involves the time elements involved with acknowledgments and time-outs of the transmitter. There is a trade-off between the time required before an acknowledgment of a segment is sent and the time a transmitter will wait for that acknowledgment before sending a segment over. Allowing the transmitter's time-out to be too short can cause congestion in the circuit since acknowledgments may not be received in time and the transmitter will retransmit the data. Allowing a transmitter timer to be too long or a receiver acknowledgment to be delayed will cause the network to act too slowly (Stallings, 1985a).

The DDN has a wide variety of networks and internetworking systems; therefore, transmitter time-outs are dynamically determined. The Round Trip Time (the time for a datagram to traverse the network plus the time for an acknowledgment to traverse the network) is determined. Next, a smoothing factor is added, since Round Trip Time will change. Next, upper and lower limits are set up based on the above information which then are computed to give an overall retransmission time-out (Transmission Control Protocol, 1983).

Acknowledgments will be generated whenever a segment is received; therefore, there is no actual computational requirement for acknowledgment. Even so acknowledgments must also take in a number of considerations. These considerations will be discussed next.

In the preceeding section, it was shown that acknowledgments are sent to show receipt of a datagram. The datagram received may be actually a segment of the entire datagram that was sent. All lower layers have been stripped out. To receive a positive acknowledgment, the segment must be undamaged and must have the correct sequence number, otherwise the segment is discarded. Discarded datagrams are then retransmitted by the transmitter. In checking for a damaged segment, TCP uses a checksum concept. "A checksum value is computed for each outbound segment and placed in the header's checksum field. Similarly, the checksum of each incoming segment is computed and compared against the value of the header's checksum field. If the values do not match, the incoming segment is discarded without being acknowledged" (Transmission Control Protocol, 1983, p.78). To detect the wrong sequence number, an octet is assigned a specific sequence number; therefore, a receiving TCP can detect duplicate and out-of-order segments (Transmission Control Protocol, 1983).

Flow Control: The flow control mechanism discussed in layer two of CCITT X.25 is similar to that used in this layer. The basic idea is that a transmitter should not send more data than a receiver can hold in its buffers. Therefore, a window size with a specific range of sequence numbers is used to denote how much data a receiver can handle in its buffers. This range is dynamic and can change as a receiver's buffer storage capacity changes. The window field of the TCP header is reserved for this function (Transmission Control Protocol, 1983). Since this window is dynamic it can change with each transmission. Normally, it is strongly discouraged to allow a window size to shrink. This happens if a receiver has a large window during the call set up, and then the buffer capacity changes to a smaller window without being able to accept data from its initial larger window. This is particularly bad since the transmitter will either have to retransmit all the data segments it is holding in queue or wait for a change in window allocation and reconfigure its permissible data window.

TCP uses a number of management techniques to deal with window sizing. The window should never be greater than the actual capacity of the receiver. This, of course, means a receiver will not accept all the data sent by a transmitter. Conversely, small windows can cause data to be transmitted in very small segments. There is no ideal size, but using 20 to 40 percent of the receiver's buffer space allows a receiver to set up a connection with a reasonable window (Trnansmission Control Protocol, 1983). A receiver can initially send acknowledgments with a small window and wait for additional buffer space before increasing its window size.

Addressing: At this layer a specific user must know the address of the destination program or entity it is trying to contact. The TCP layer provides the lower layers with a global addressing scheme (Transmission Control Protocol, 1983). This global addressing scheme is either known by the user or the user can use a directory provided by the network being used. The DDN supplies well known addresses and a directory address of individuals using the network. The actual source port or user port must be sent to the destination port at this layer. The network and local addressing schemes were covered in the section on IP layer.

4.2.3 TCP Services

TCP provides additional services that are used at this layer. These services do not have particular problem areas in this layer but are an integral part of TCP. The services are: multiplexing and data transport. These services are discussed next.

Multiplexing services: A number of user parts can be serviced at one time from a particular host. Also, a number of ULP's can use TCP simultaneously. Using a destination port identifier allows TCP to determine where a particular segment should go. Port identifiers are selected by each TCP and, together with an internet address, form what is called a socket (Transmission Control Protocol, 1983). This socket is the unique name of a ULP within the internet. In this way, simultaneous users can be serviced by TCP.

Data transport services: Once a connection has been made, TCP must provide for the flow of data across that connection. Some of these mechanisms have already been discussed, such as flow control and error checking. The remainder of the data transport services are full-duplex, ordered data flow, labeled services, data stream push, and urgent data signaling. A brief description of each follows:

1) Full-duplex Capability - TCP supports the simultaneous bi-directional data flow between connected ULP's;

2) Ordered Data Flow - TCP must deliver the data it receives in sequential order. IP is not required to transmit datagrams sequentially since it is a connectionless service. TCP accounts for this and puts the data in proper sequence before delivering it to an ULP;

3) Datagram Labeling - TCP is required to label the levels of security and precedence of its calls during connection establishment. These levels are provided by the ULP's. If the ULP does not supply the information, a default value is assigned by TCP;

4) Data Stream Push - Normally TCP can hold data until enough has been received to create a full segment. When the push flag in an incoming TCP header segment is activated, the TCP layer is required to pass that information without waiting for more;

5) Urgent Signaling - When significant information is being delivered, the urgent flag in the incoming TCP header segment is set to one. This informs the ULP that urgent information is forthcoming. To enhance this service the push flag is usually set in conjunction with the urgency flag (Transmission Control Protocol,

1983).

That concludes the discussion on DOD's IP and TCP. To establish a good comparative study, the industry protocols must also be addressed. The following sections cover ISO's OSI Reference Model using the draft standard Connectionless-mode Network Protocol and the established Transportt Protocol.

4.3 Connectionless-mode Network Protocol

ISO's draft International Standard (DIS 8473) is a computer protocol standard designed to be used as an interconnecting protocol in the network layer. This protocol is called the Connectionless-mode Network Protocol (CLNP). The concept of CLNP is the same as the DOD's IP; that is, it will interlink separate networks and provide a connection-less service (DIS 8473). The functions and characteristics of CLNP are similar to IP, but there are structural differences between the two protocols. Also, IP has evolved and incorporated a number of other protocols for the management of internetworking separate networks. These protocols are the Internet Control Message Protocol (ICMP) and the Gateway-to-Gateway Protocol (GGP) which have already been discussed. ISO is beginning to address some of these management functions and is presently determining what additional protocols are needed when using CLNP (D.Walters, personal communication, November 1985).

4.3.1 CLNP Structure

CLNP uses protocol data units (PDU's) that are octet aligned and, like the rest of the protocols discussed, each PDU has a header. The header is broken down into five specific parts. They are the fixed part, the address part, the segmentation part, the options part, and the data part. Each part has its own set of fields. Figure 4.6 shows a CLNP header for a typical DPU. This section gives a brief description of each part and the fields associated with those parts. Included in the description is a comparision between the DOD's IP header and ISO's CLNP header.

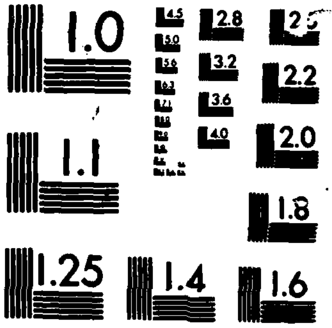
The following is a brief description of the fixed part in CLNP:

1) Network Layer Protocol Identifier - This field identifies the Network Layer Protocol as ISO 8473. This field is fixed at one octet and is given the binary value of 1000 0001. DOD's IP does not have such a field;

2) Length Indicator - This field gives the header length in octets and is one octet in length. The IP Internet Header Length (IHL) is only four bits

AD-A167 052 SELECTED COMPARISONS OF DEFENSE PACKET SWITCHING VS COMMERCIAL DATA COMMUNICATIONS PROTOCOLS(U) AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH J E TARANTINO 2/2

UNCLASSIFIED 1985 AFIT-CI-NR-86-57T F/G 17/2 NL



MICROCOP   CHART

Network Layer Protocol Identifier
Length Indicator
Version / Protocol ID Extension
Lifetime
SP MS E/R Type
Segment Length
Checksum
Destination Address Length Indicator
Destination Address
Source Address Length Indicator
Source Address
Data Unit Identifier
Segment Offset
Total Length
Options
Data

Figure 4.6 Connectionless-mode Network Protocol

Source: ISO/DIS 8473 (Revesed), 1985

in length but has the same function;

3) Version/Protocol Identifier Extension - The value of this field is 0000 0001, and denotes the use of the standard version of ISO 8473. There is also a version field in IP which is four bits in length;

4) PDU Lifetime - As in IP, CLNP has a set lifetime for a data unit (packet). The lifetime field is encoded as a binary number in units of 500 milliseconds. It is decremented each time a network-entity processes the PDU. The lifetime of the PDU will also decrease (called life-time delay) if the sum of the delay within the system is more than 500 milliseconds. This lifetime delay function is an added feature that is not found in IP. IP only has an IMP hop function called time-to-live;

5) Flags - There are three flags used in the CLNP header. They are a segmentation permitted (SP) flag, a more segmentation (MS) flag, and an error reporting (E/R) flag. The first two flags are also used in IP. Error reporting for IP is done by a separate protocol called the Internet Control Message Protocol (ICMP);

6) Type Code - This field identifies the type of protocol data unit being sent by a transmitter.

Two types of PDU's are allowed, a Data Protocol Data Unit (DT PDU) and an Error Report Protocol Data Unit (ER PDU). Again, DOD's ICMP handles error reporting in the form of diagnostic packets;

7) Segment Length - This field is used when a PDU has been segmented, and gives the length of the entire segment including both header and data. When a PDU is not segmented, the value of this field is the same as the value of the Total Length field. Of course, IP has a similar function for fragmenting packets;

8) Checksum - As with IP, there is a 16 bit checksum that computes the packet header bits for errors (DIS 8473).

This ends the definitions related to the fixed part of a PDU header. This next list contains the address part of a PDU header:

1) Destination Address Length and Source Address Length Indicators - Both indicators specify the length of the destination or source address by giving the number of octets of each address. These indicators do not exist in IP because the source and destination addresses in IP are a fixed length of 32 bits;

2) Destination and Source Address - These fields are

variable in length depending upon the actual network service access point address (DIS 8473).

That concludes the definitions of the address part. The next list contains the segmentation part of the CLNP header:

1) Data Unit Identifier - This field identifies an initial data unit that has been segmented. Marking the initial data unit allows the rest of the segments to be put back together by the destination network-entity. IP uses an identification field that also marks the segmented packets;
2) Segment Offset - As in IP, this field identifies the relative position of the segments in relation to the rest of the segmented packet;
3) Total Length - This field specifies the total length of the initial data unit(DIS 8473). IP also has a Total Length field.

4.3.2 CLNP Options

The final field covered in this section is the option field. This field allows for the following six options: padding, security, source routing, recording of route, quality of service maintenance, and priority. Since these options are functionally the same as IP, they will not be discussed again.

4.4 ISO Transport Protocol

ISO's Transport Protocol (TP) is far more complex than ISO's CLNP. It is also far more advanced in its design and acceptance. Since the CCITT has adopted the OSI Reference Model, the comparative study uses CCITT X.224.

CCITT X.224 defines five classes of protocols at the transport level. These classes are:

1) Class 0: Simple Class;
2) Class 1: Basic Error Recovery Class;
3) Class 2: Multiplexing Class;
4) Class 3: Error Recovery and Multiplexing Class;
5) Class 4: Error Detection and Recovery Class (CCITT X.224, 1985).

The type of class used depends on the lower layer services that are available to the transport layer. Since DOD's IP is an unreliable service because it lacks flow control and end-to-end acknowledgments, it requires the use of the Class 4 TP (Stallings, 1985a). Therefore, TP-4 was used in the comparative study with the DOD's TCP. TP-4, as with TCP, is an end-to-end protocol that is connection orientated, providing services that are functionally similar to TCP (Committee, 1985). The structure and functions of TP-4 are viewed first, followed by a study that analyzes the differences between the two protocols.

4.4.1 Structure of TP

There are a number of header structures used in this protocol. A typical structure of a Connection Request (CR) packet is shown in Figure 4.7. A brief description of each field is given below:

1) LI - The length indicator field has a maximum value of 254, 11111110. This indicates the header length in octets including parameters. The length indicator does not include the length indicator field itself or the user data field. This indicator points to the beginning of the data field and is similar to the Data Offset field in TCP;

2) CR - The Connection Request Code field is a predetermined code to denote which type of Transport Protocol Data Unit (TPDU) is being sent. 1110 stands for CR-TPDU. TCP uses a SYN code for its connection request in the flag field;

3) CDT - The CDT field is a Credit field used for initial credit allocation for the receiver. It is a flow control mechanism in the receiver for receiver-to-transmitter data exchange. TCP also

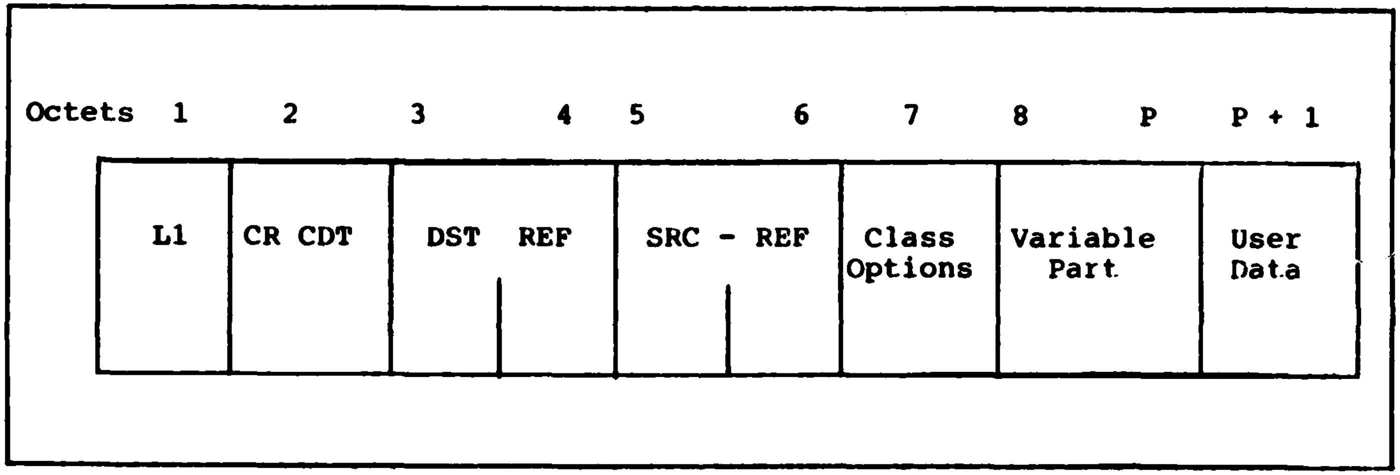


Figure 4.7 Connection Request Packet

Source: CCITT X.224, 1985

uses a credit window field;

4) DST-REF - In the destination-reference field, octets 3 and 4 are set to zero;

5) SRC-REF - The Source-reference field is the source reference selected by the transport entity that has asked for a CR and identifies the requested transport connection. This is not an addressing function but only a reference for mapping;

6) Class, Options - This field is a one octet field. Bits 8-5 show the class of operation, 0100 is class 4. Bits 4-1 define the options present in the TPDU. (CCITT X.224, 1985).

The variable part will be taken separately since this field provides the bulk of parameters used in a Transport Protocol Data Unit. Some of the parameters used in the variable part must be set up during the call connection and can not be changed during the entire length of the call. The following list contains all the elements of the variable part:

1) The Transport service access point identifier (TSAP-ID) is used for addressing during the connection request;

2) The TPDU size parameter is a one octet parameter that gives the length of the TPDU. The maximum length of a TPDU is 8192 octets including the

header. The DDN also uses a user data packet of 8192 maximum octets in length, but at the data link layer (BBN, 1983);

3) The Version Number parameter is set to show which version is being used. Presently, it is set to one. The version field is not found in the DOD's TCP but in the DOD's IP;

4) A Security Parameter is available and is user defined. TCP uses a datagram labeling function to provide the security and precedence levels;

5) The checksum function is available for Class 4 operation. TCP also provides a checksum function;

6) The Additional-options-select parameter allows for the selection of more options, such as a 16-bit checksum in Class 4 operation, or the use of expedited data service. The push flag and urgency flag in TCP also allows for expedited service;

7) The Alternate-protocol-classes parameter is a binary number representation of the class used;

8) The Acknowledgment time parameter is used only in Class 4 operation. This parameter shows the maximum acknowledgment time to a remote transport entity. It is two octets in length and states the time in milliseconds. The DOD's IP layer

provides for time stamping of datagrams as they traverse the network;

9) The Throughput field can be anywhere from 12 to 24 octets in length. There is a maximum throughput stated in the first 12 octets and an average throughput stated in the second 12 octets. DOD's IP provides for a high or low throughput option;

10) The Residual Error Ratio parameter is a 3 octet parameter and appears to be similar to the DOD's IP reliability parameter;

11) The priority field is two octets in length and also appears to be similar to the precedence option in DOD's IP;

12) The transit delay field is eight octets in length;

13) The Reassignment Time parameter states the Time to Try Reassignment/Resynchronization (TTR). It is a two octet field;

14) The Used Data field can not exceed 32 octets in the RC packet but has a maximum length of 8192 octets as stated before (CCITT X.224 ,1985).

4.4.2 TP-4 Characteristics

There are specific procedures used in the operation of TP-4 just as in the operation of TCP. The problems associated with the transport layer were covered during the discussion of TCP. Therefore, only the actual functions of TP-4 will be covered and not the problems. The characteristics discussed in this section are: connection establishment and termination, retransmission and acknowledgments, flow control, and data transfer.

Connection establishment and termination: The connection establishment function is similar to TCP in that a three-way data exchange (or handshake) takes place. That is, the sender of a connection request must respond to a connection confirmation from a remote entity with some form of acknowledgment. This acknowledgment can take the form of a data unit, an expedited data unit, a disconnect request, or an actual acknowledgment (CCITT X.224, 1985). The termination function in TP-4 is not as graceful as in TCP. There is only an immediate disconnect service in TP-4.

Retransmission and acknowledgments: As with TCP, the times for transmission, acknowledgment, and retransmission are critical at this layer. TP-4 uses specific formulas to determine how long a transmitter should wait before retransmitting its data. Also, there is a maximum number of retransmissions allowed just as in TCP.

Flow control: The window mechanism in TP-4 is dynamically adjustable as was in TCP. A credit system is used where the transmitter is allocated so much buffer space on the initial call set up. As the transmitter transmits each unit, it reduces its window by one unit. When the receiver acknowledges the unit, it will renew the credit of the transmitter by the number of units it has accepted. Therefore, as buffer space changes, so can the credit limits of the receiver (Stallings, 1985a).

Data transfer: Data transfer takes place in a normal mode or it can be expedited. Either way, during the data exchange all data units must be delivered in the order they were sent. A numbering sequence of the data unit is used. This numbering squence also helps establish the window size of operation for the flow control mechanism. A data transfer unit has its own format. Figure 4.8 shows the normal structure of a data unit for class 4 operation (CCITT X.224, 1985).

The fields of a data unit are similar to most of the fields of a Connection Request Unit; therefore, only the different fields will be discussed. The following list defines those different fields:

1) The data transfer code denotes that the unit is a data unit;
2) The Transport Protocol Data Unit Number (TPDU-NR) is the send sequence number that is the number associated with that data unit;

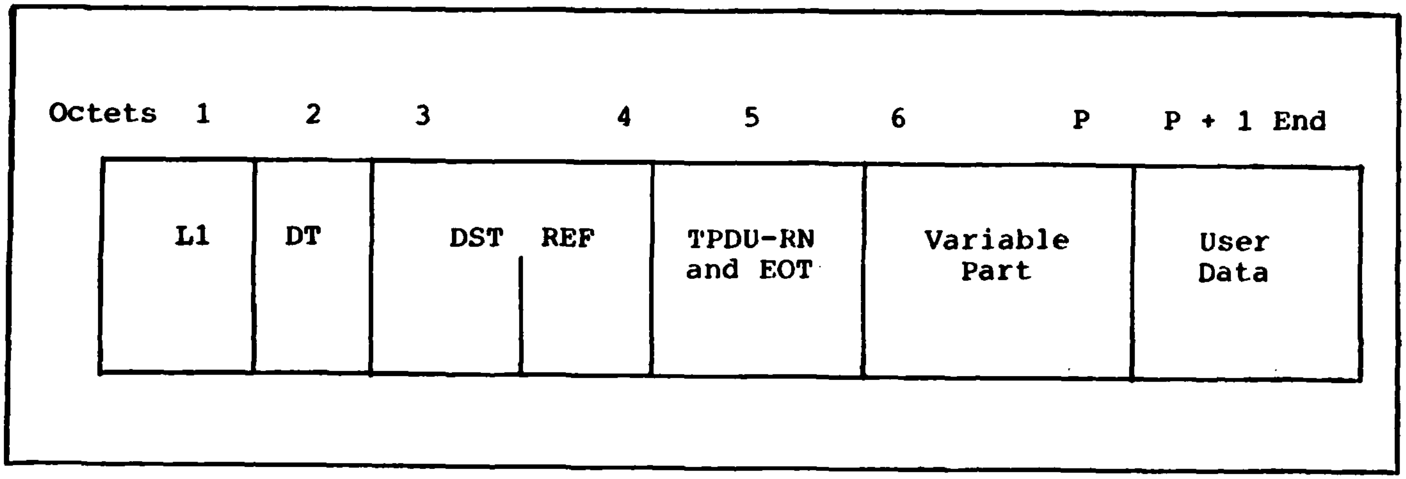


Figure 4.8 Data Transfer Packet

Source: CCITT X.224, 1985

3) End-of-Text (EOT), when set to one, denotes the last data unit of a complete TPDU sequence (CCITT X.224, 1985).

Of the fields mentioned above, TPDU-NR is the only one which is similar to TCP. TCP uses a sequence number method. The other fields are not found in TCP.

During the data transfer, acknowledgments are sent back and forth. Acknowledgments, also, have their own format or header. The major difference in a data unit and an acknowledgment (AK) unit is in octet five. This octet has a "YR-TU-NR" (your-turn-next) field which indicates the next expected DT-TPDU number (CCITT X.224, 1985).

This section has outlined the structure and functions of ISO's TP-4. There are a great number of similarities between the two protocols especially from a functional user's standpoint. But there also remains a number of differences which make these protocols incompatible. The comparative study deals with those differences.

4.5 Comparative Study Between DOD's IPPand TCP and ISO's CLNP and TP-4

The DOD requires the services of TCP/IP because these protocols fill some unique DOD needs. These needs can be broken down into six operational areas. They are survivability, security, precedence, robustness, equipment availability, and interoperability. The comparative study looks at these needs from two perspectives. First, the differences in design features of the protocols will be compared. All of the similarities have already been covered and will not be mentioned again. Then, the comparative study determines whether ISO's TP-4 and CLNP can actually fill the needs of the DOD in the six operational areas mentioned. This second concept is critical in determining not only what the differences in the protocols are, but also if the DOD could even migrate to the OSI architecture. The next four sub-sections cover some of the technical differences in the protocols.

4.5.1 Addressing

As seen before, TCP provides a four octet length address. This addressing format has four variable classes for use in the network and local addressing schemes. IP then examines these addresses to determine where a datagram should be sent.

TP-4 provides a variable-length address called TSAP-ID in the call request unit. The addressing concept in TP-4 is still an open area for discussion; therefore, there may be changes in its format structure. The impact of this difference is still not completely known but should be minimal (Committee, 1985).

4.5.2 Data Transfer

In the previous discussion on TCP, it was noted that TCP is stream-orientated. This method does not deliver an End-of-Text (EOT) but rather a one bit, FIN, code in the flag field. Also, TCP accepts a push on the send side if required. TP-4 is different in that it is block-orientated. The use of an EOT is similar to a TCP push. Because of these differences, some modification of the protocols would be required to make them compatible.

4.5.3 Flow Control

There is a big area of difference between TCP and TP-4. Although TCP has a similar dynamic window sizing as does TP-4, TCP uses an octet allocation, while TP-4 uses a segment allocation. Both methods were developed to provide good flow control for the type of data transfer they employ. Therefore, any changes in the methods used, stream versus block, will require extensive changes to the flow control mechanisms of the protocols (Committee, 1985)

4.5.4 Error Reporting

Error reporting in ISO IP uses a separate packet. This method is similar to a diagnostic packet in CCITT X.25's packet layer. The DOD's IP uses the Internet Control Message Protocol (ICMP), which is a completely separate protocol for this management function.

As can be seen, these basic differences are more in design than in functionality. Of course, these differences make the protocols incompatible. The following six sub-sections determine whether or not ISO's protocols, CLNP and TP-4, can meet the DOD's present needs. Recall that the six needs covered in this thesis were survivability, equipment availability, robustness, security, precedence, and interoperability. The following sub-sections discuss each DOD need separately.

4.5.5 Survivability

The concept of survivability is a function of redundancy considering that, if many modes are destroyed, the networks involved can still continue to operate. The DDN has many interlinking modes, and the type of protocol used (DOD's IP or ISO's CLNP) within this system will not really matter. But the DOD would like to use civilian networks if the DOD's systems have a catastrophic failure. The problem here becomes one of interoperability; that is, if civilian systems migrate to the OSI model the DOD will not be able to interoperate with those networks. The use of TP-4 could actually enhance the survivability needs required by the DOD and the DDN.

4.5.6 Equipment Availability

The concept of equipment availability is such that as systems fail, the parts for those systems must be readily available. It becomes obvious that the more vendors supporting the DOD's protocol, the more available parts will become. The DOD's TCP/IP protocols are not being adopted by the computer industry; therefore, availability of parts may get worse as the DDN and other DOD networks get older. This concept also covers supportability and maintainability, those areas not independently covered by this thesis. The further away the DOD aligns itself from industry, the more the factors mentioned above are affected. Again, ISO's CLNP and TP-4 will add to the concept of availability, especially as the DOD networks age.

4.5.7 Robustness

Robustness deals with the ability to transmit datagrams in a changing topology. DOD's IP provides for a robust design. It would appear that a protocol based on the DOD's IP, such as OSI's CLNP, can continue to provide the robustness needed by the DOD.

4.5.8 Security

The security is paramount in DOD networks such as the DDN. The DDN is to provide the backbone Command, Control and Intelligence for the DOD. The use of TP-4 is considered sufficiently equivalent to TPC (Committee, 1985).

4.5.9 Precedence

Another unique DOD requirement is precedence. The ability to preempt a lesser priority call, in place of higher priority information, is critical within DOD networks. Both the DOD's TCP/IP and ISO's CLNP and TP-4 support adequate precedence ratings.

4.5.10 Interoperability

Interoperability is a major concern of the Government and the DOD (Committee, 1985). Interoperability can be viewed from two major areas in computer architecture. First, the lower layer protocols must conform to similar standards to achieve interoperability. The third chapter of this thesis showed that the Government and the DOD have already moved toward the implementation of CCITT's X.25 involving the DTE to DCE interface. The other area of interoperability is at the application or highest layer. Having application programs that are interoperable is the key to true interoperability. This thesis does not cover application layers, but application layers used in the DDN must use TCP/IP. Any application programs that do not use TCP/IP are not interoperable with other programs. This factor again brings the DOD away from standardized application programs that will be supported by vendors in the upcoming years. The use of TP-4 will allow better interoperability with off-the-shelf programs in the next decade and probably beyond.

These major operational needs are not the only concepts that should be discussed. The financial ability of the DOD to support particular systems that use unique protocols must be a major consideration when comparing protocol designs. Another key area of concern that is paramount to DOD's future needs is the concept of adopting and using technical advancements as they come about. These two areas are covered separately to determine the impact of using TCP/IP or CLNP and TP-4.

4.5.11 Affordability

Obviously, the more specific and unique a system becomes, the more expensive it can get to maintain and change. As more and more vendors begin to support the OSI model, the DOD's networks will become more and more unique. This factor alone will drive the price of supporting the system higher, since the use of a commercially developed product supplied by many vendors tends to be cheaper.

4.5.12 Technological Advancement

A final factor which is an indirect need of the DOD and should be considered when comparing protocols is the concept of being able to adapt to technological advancements. As technology advances, the DOD must have a way to react to those advancements and be able to adopt the ones that enhance the DOD's systems. There is a vehicle that is already in place, that is the established international organizations, such as ISO and CCITT. The DOD should begin to play a more active role in these international standards organizations through the U.S. participants, such as NBS, ANSI and IEEE (Committee, 1985). Although initial standards take awhile to develop (as was stated in Chapter 3), the changes to these standards happen more quickly. Also, many companies consider adopting these standards even in their draft stages. This is because draft standards reach a certain point in their development and from that point on only minor changes occur in the standard. The DOD should be able to keep up with and implement the changes as they occur using off-the-shelf vendor support.

The comparative study has shown that the DOD requirements can be met using international standards. The next section rates these DOD needs on a priority bases to show which needs should be filled first.

4.6 Rating of DOD Requirements

This section contains a list of DOD requirements or needs that have been evaluated as to the importance they have in relationship to each other. The rating contains a definition of the need and a reason for the rating. The ratings follow below.

Survivability - The ability of a system to operate even if many of its component parts are distroyed.

Rating - 1: If the equipment does not survive, the rest of the concepts being evaluated are useless;

Technical advancements - The ability to adapt and use new technologies without a complete redesign of equipment.

Rating - 2: U.S. Forces must be able to maintain a superior edge over enemy forces; technological advancements play a major role in maintaining that edge.

Interoperability - To be able to interconnect many computerized battle force systems, so that vital information in one system can be used by another system.

Rating - 3: This concept is important because the idea can reap incredable benifits, but the concept has many years of work and, of course, the use of standards by the DOD.

Security - The ability to protect information from enemy forces in whatever system is being used.

Rating - 4: The DOD knows there is a threat and knows that information that is passed on the system must be authenticated; therefore, the DOD guards well against this problem. Any system used by the DOD must have this capability available in its software design.

Equipment Availability - When a system goes down for repair, equipment must be readilly available to bring that system back up to operational status.

Rating - 5: The factor is critical during two time periods. First, when the system is new and there are many equipment failures there may not be enough replacement parts. Second, when the system is in its final stages of usefulness, equpment will again become scarce.

Robustness - the ability to transmit datagrams in a changing topology.

Rating - 6: This rating is important because the threat or loss of equipment in a military environment is real. IP provides the robustness required by the DOD, as compared to a virtual circuit configuration.

Precedence - The ability to pass vital information ahead of lesser important information.

Rating - 7: This concept although important is not rated highly because special systems can be built to carry extremely vital information, therefore bypassing the need for a precedence level.

Affortability - Basically the ability of the DOD to purchase new systems, then to maintain and support those systems.

Rating - 8: If a system fills the rest of the DOD needs, then this factor should be concidered last. This rating hinges on the DOD using off-the-shelf vendor equipment and not specifically designed systems.

This concludes the rating of each DOD requirement and concludes this chapter. The last chapter is the conclusion sought by this thesis.

CHAPTER V

CONCLUSION

The overall concept of this thesis has been to examine some functional differences between the DOD and industry protocols. A comparative study between particular protocols was used to determine how far apart the DOD was from industry standards, and if the DOD had unique requirements that were increasing procurement complexities and overall system cost.

This thesis considered three protocols used by the DOD in the Defense Data Network and three similar protocols used in industry. In the first comparision it was seen that the access protocol used in the DDN, X.25, is based on the international standard X.25 developed by the CCITT. The CCITT X.25 standard has become widely accepted in industry; therefore, many products available today are compatible with it. In using this protocol, the DOD has enabled itself to use off-the-shelf designs or at least designs that require only minor modification to their software packages. In this way the DOD has helped to decrease procurement times and overall system costs for its access products. However, the second comparative study between DOD's Internet Protocol (IP) and Transmission Control Protocol (TCP) and ISO's Connectionless-mode Network Protocol (CLNP) and Transport Protocol level 4 (TP-4) shows that the DOD is moving away from protocols that are being designed and implemented in the computer industry. Also, because the NBS has worked in the design of these international protocols, the DOD has separated itself from the rest of the Government in terms of protocol design.

The present impact on procuement cycles and overall system costs to the DOD in its use of IP and TCP (TCP/IP) is minimized because the OSI model is not fully developed. But once the model is integrated into a working computer architecture, the impact will be greater. There are three major reasons for this impact. First, DOD's sunken costs in TCP/IP may be too large to allow it to make a realistic change to CLNP and TP-4. These sunken costs may also dramatically increase as the DOD's networks age. Next, vendor support for international standards has grown at a tremendous rate, and it is estimated that by the mid-1990's only two computer network architectures will remain. They are IBM's SNA and the OSI Reference Model (Passmore, 1985). Finally, a major study was done by the Committee on Computer-Computer Communications Protocols, specifically aimed at comparing the DOD's TCP/IP with the ISO CLNP (called the Internet Protocol in the computer study) and TP-4. This study shows that the protocols are functionally the same and can meet DOD requirements. The study also shows some major impacts if the DOD continues to use TCP/IP, some of which were used in this thesis. The report by the committee suggested three options for the DOD in determining whether to use TP-4. The evidence from this study was overwhelmingly in support of option one. This option called for the DOD to "immediately modify its current transport policy statement to specify TP-4 as a costandard along with TCP" (Committee, 1985, p. 45). Even option two stated the DOD should "immediately announce its intention to adopt TP-4 as a transport protocol costandard with TCP after a satisfactory demonstration of its suitability for use in military networks" (Committee, 1985, p. 45). The final option was the one selected by the DOD. The DOD's official guidelines for implementing TP-4 is that they will not utilize it until it is fully operational and supportable within private industry (V. Russel, personal communication, August, 1985). The problem with the DOD waiting for industry to use TP-4 is that private industry may not have a need for TP-4. This is because TP-4 has been developed for use with ISO's CLNP which is a connectionless service, and most industry networks are using virtual circuit designs. Therefore, the DOD may find itself waiting a long time for technical advanced protocols that are already available.

A final point to be made in this thesis is that Government regulations are beginning to require the use of international standards when feasible and before too long, the DOD may be required to adopt ISO's IP and TP-4. This appears to be the best solution to the considerations brought up in this thesis. That is, the solution is to require the adoption of international standards through regulation, thereby eliminating different departments within the government from having their own separate computer designed networks. Therefore, the DOD should not have been given three options in the NRC report (1985). Instead adoption of ISO's IP and TP-4 should be mandatory. This concept will help to lessen the impact of many of the considerations covered in this thesis and help drive the Federal Government toward a more unified position in computer architectures.

BIBLIOGRAPHY

Air Force information systems architecture. (1985). Washington, DC: Department of the Air Force.

BBN Communications Corporation. (1983). Defense data network X.25 host interface specification (Research Rep. No. AD/A137 427). Cambridge, MA: Author.

Beauchamp, K. G. (Ed.). (1979). Interlinking of computer networks. Dordrecht, Holland: D. Reidel.

Bolt Beranek and Newman Inc. (1981). Specifications for the interconnection of a host and an IMP (Research Rep. No. 1822). Cambridge, MA: Author.

CCITT V.35. (1981). Yellow Book, Vol. III. Data transmission at 48K bit/s using 60-108K hz group circuits. ITU Geneva.

CCITT X.25. (1984). Document AP VIII-58-E. VIIIth Plenary Assembly, June 1984.

CCITT X.224. (1985). Red Book, Vol. VIII. Transport protocol specifications for open system interconnection for CCITT applications. ITU Geneva.

Cerf, V. G., & Cain, E. (1983). The DoD internet architecture model. In W. Stallings, Tutorial: Computer communications: Architectures, protocols, and standards (pp. 79-89). Silver Spring, MD: IEEE Computer Society Press.

Cerni, D. M. (1984). Standards in process: Foundations and profiles of ISDN and OSI studies. (NTIA Report 84-170). U.S. Department of Commerce: National Telecommunications and Information Administration.

Clark, G., & Wong, M. K. (1985, April). Verifying conformance to the X.25 standard. *Data Communications*, pp. 153-161.

Committee on Computer-Computer Communication Protocols. (1985). *Transport protocols for Department of Defense data networks*. Washington, DC: National Academy Press.

Defense data network. Defense Communications Agency. Unpublished raw data.

Defense data network newsletter. (November 1984 - April 1985). Washington, D.C.: Defense Communications Agency.

Defense data network program management plan. (1984). Washington, DC: Department of the Air Force. Unpublished raw data.

DIS 8473. International Organization for Standardization.

Electronic Industries Association. (1969). *Interface between data terminal equipment and data communication equipment employing serial binary data interchange* (Research Rep. No. RS-232-C). Washington, DC: Author.

FIPS PUB 100/Federal Standard 1041 (1983). *Interface between data terminal equipment and data circuit-terminating equipment for operation with packet-switched data communications networks*. Washington, DC: National Bureau of Standards.

Glen, D. V. (1985). *Local network assessment*. (NTIA Report 85-174). U.S. Department of Commerce: National Telecommunications and Information Administration.

Hurlbut, J. H. (1984, June). An approach to integrating defense data communications. *Government Executive*, pp. 62-64

Minden, R., Haverty, J., & Sheltzer, A. (1983, September). The DARPA internet: Interconnecting heterogeneous computer networks with gateways. In W. Stallings, *Tutorial: Computer communications: Architectures, protocols, and standards* (pp. 231-241). Silver Spring, MD: IEEE Computer Society Press.

Ingram, W. (1985). Draft - Differences between 1980 and 1984 X.25. Unpublished raw data.

Internet protocol. (1983). (Standard No. MIL-STD-1777). Washington, DC: Department of Defense.

McNamara, J. E. (1982). Technical aspects of data communications (2nd ed.). Bedford, MS: Digital Equipment Corporation.

Mitre Corporation. (1983). Defense data network subscriber interface guide (contract No. F19628-82-C-0001). McLean, Virginia: Author.

Mitre Corporation. (1984). Defense data network system description (Contract No. F19628-84-C-0001). McLean, Virginia, Author.

Padlipsky, M. A. (1983). A perspective on the arpanet reference model. In W. Stallings, Tutorial: Computer communications: Architectures, protocols, and standards (pp. 91-102). Silver Spring, MD: IEEE Computer Society Press.

Passmore, L. D. (1985, February). The networking standards collision. Datamation, pp. 98-108.

Postel, J. (1980). Internetwork protocol approaches. In W. Stallings, Tutorial: Computer communications: Architectures, protocols, and standards (pp. 223-230). Silver Spring, MD: IEEE Computer Society Press.

Postel, J. (1985, May). A DoD statement on the NRC report. (Available from Assistant Secretary of Defense, Washington, DC, 20301 - 3040).

Simple mail transfer protocol. (1984). (Standard No. MIL-STD-1781). Washington, DC: Department of Defense.

Stallings, W. (1984, November). A primer: Understanding transport protocols. Data Communications, pp. 201-215.

Stallings, W. (1985a). Data and computer communications. New York: Macmillan.

Stallings, W. (1985b). Tutorial: Computer communications: Architectures, protocols, and standards. Silver Spring, MD: IEEE Computer Society Press.

System Development Corporation. (1982). DoD protocol reference model (Research Rep. No. 7172/201/01). Santa Monica, CA: Author.

Tanenbaum, A. S. (1981). Computer networks. Englewood Cliffs, NJ: Prentice-Haall.

Telnet protocol. (1984). (Standard No. MIL-STD 1782). Washirgton, DC: Department of Defense.

Transmission control protocol. (1983). (Standard No. MIL-STD-1778). Washington, DC: Department of Defense.

END
FILMED

5-86

DTIC